

Open Internet for Democracy Leaders

Submission to the Global Digital Compact

Introduction

Democracy relies on the free flow of ideas, which in the modern age means having an open and inclusive internet that allows citizens to freely share their opinions, exchange ideas, and engage in public debates and interactive dialogue. Access to an open and inclusive internet is necessary to strengthen democratic engagement and governance, promote social accountability, and enable equal participation in the market economy.

Given increasing global reliance on the internet, we believe that the UN Global Digital Compact should focus on how an open and accessible internet is fundamental to the success of democratic societies worldwide. An open and inclusive internet enhances democratic processes in the following ways:

- Increases access to information, including news, analysis, and research, that can help individuals make more informed decisions in the democratic process.
- Strengthens political engagement by enabling individuals to easily contribute to political discussions and debates with others, regardless of geographic location.
- Improves transparency in government decision-making by providing a platform for government agencies and officials to share information with the public in real-time.
- Encourages civic participation by allowing individuals to easily find and connect with community groups, political parties, and advocacy organizations that align with their interests and values.
- Fosters government accountability by enabling individuals to easily track the actions and decisions of government officials, including voting records, campaign contributions, and other relevant information.
- Enables remote voting in some cases, which can increase accessibility and participation in the democratic process, particularly for individuals who have mobility or accessibility issues, or who are living in remote or rural areas.

While noting the importance of the internet in democratic societies, we also need to acknowledge existing online threats and harms, including the continuous violation of human rights online, attacks on information integrity, cybercrime and data breaches, violence against women online, as well as widening gaps in the digital divide. These challenges, among others, have impeded the advancement of democratic participation both online and offline.



In the pursuit of outlining shared principles for an open, free, and secure digital future for all that protects democracy in the digital age, this submission focuses on the following thematic topics and the ways in which they intersect with democratic norms and values:

1. Apply Human Rights Online
2. Avoid Internet Fragmentation
3. Digital Commons as a Public Good
4. Protect Data
5. Regulation of Artificial Intelligence

Multistakeholderism has proven to be the most effective model for internet governance and accountability. There must be action and adherence from all digital actors, both public and private, in order to secure a free and inclusive internet that benefits all of humanity. Given the vital importance of multistakeholder participation in the development of global norms and standards that help shape the future of the internet, this document outlines how diverse stakeholder groups can work together to protect democracy in the digital age. Under each key theme, we provide recommendations on how stakeholder groups such as government, civil society, media, and the private sector can engage with one another to ensure the advancement of a democratic digital space.

We welcome the opportunity to contribute our input to the Global Digital Compact. Our goal is to share experiences from grassroots communities, democratic reformers, youth, and other stakeholders who have been working to advance digital rights.



Description of the Submitting Organization

This submission is the work of the 2022-2023 cohort of [Open Internet for Democracy Leaders](#), a unique cohort of global advocates from civil society, media, and the private sector who possess an unwavering commitment to safeguarding and advancing the principles of an open internet.

This document reflects our deep thinking and nuanced perspectives on the high-level issues for which the Secretary General has requested feedback. We have utilized our extensive knowledge and expertise to carefully synthesize and summarize our thoughts on these critical matters.

To provide a comprehensive and informed response, we have also engaged with our networks working on internet governance topics, to capture additional insights and perspectives. By incorporating their feedback into our submission, we have enriched the breadth and depth of our analysis, ensuring that our response is both inclusive and reflective of diverse perspectives.

Through our submission, we seek to contribute to the global discourse on the open and democratic internet, advocating for its continued protection and promotion. We believe that an open internet is essential to the realization of fundamental human rights, the promotion of democratic values, and the advancement of social, economic, and cultural progress. As such, we are honored to present our submission to the Secretary General, and we remain committed to working tirelessly towards the preservation and advancement of an open and democratic internet for all.

Apply human rights online

Overview

Human rights are important for democracy because they are the foundation of individual liberty and dignity, and they establish the basic conditions necessary for people to live freely and participate fully in democratic societies. While digital technologies and the internet are propelling exceptional human progress, ensuring adherence to human rights principles in the online space is crucial to the protection of democracy in the digital age. Closing the digital divide is also important to ensure that every person across the globe is able to exercise their human rights.

Key principles

- Guarantee the rights that people have offline are also protected online
- Human rights are a fundamental building block for democratic societies
- Achieve universal access to the internet and bridge digital divides
- Promote equality and meaningful access to the internet

Recommendations

Governments:

- Ensure existing and new policies, regulations, and frameworks acknowledge digital rights as human rights
- Build the capacity of government agencies and the judiciary to resolve digital rights issues and provide recourse for human rights violations online
- Take a human-centric approach, focusing on end-users and communities when developing policies on human rights online
- Ensure identity-based harassment and bullying of vulnerable and minority groups on the internet are recognized as hate crimes, and receive appropriate protections including legal redress as per local hate crime laws

Civil Society:

- Build the capacity of broad civil society actors not already actively engaged in digital rights discussions to understand the importance of promoting human rights online
- Collaborate with other stakeholders like the private sector and technologists to develop laws and policies that promote and protect online human rights
- Develop public awareness campaigns to assist people in recognizing human rights issues online and educate them on pursuing appropriate measures to seek redressal
- Monitor and document online human rights abuses or violations carried out by governments, private sectors and individuals

Private Sector:

- Collaborate with diverse stakeholders including academia, civil society, media, and artists to develop business policies that protect human rights online
- Establish diverse private-public partnerships and build coalitions that amplify efforts to promote and secure human rights online
- Technology companies should collaborate with stakeholders such as law enforcement agencies, government, social workers, academia, and civil society to develop mechanisms that review and address human rights violations cases reported across their platforms
- Ensure that technologies or platforms developed for either commercial or non-commercial purposes adhere to human rights principles, and are inclusive, accessible, and secure

Media:

- Report and investigate human rights violations taking place online or being facilitated by digital tools
- Collaborate with civil society to investigate human rights violations online, and promote factual reporting on these investigations
- Support training for journalists to enhance their comprehension of technological advancements and their socio-economic implications

Avoid internet fragmentation

Overview

The global democratic potential of the internet can only be realized if all citizens around the world have access to an open, interoperable network. The internet is a platform for citizens to access diverse views and opinions and also to create deeper social engagements and mobilize. Internet fragmentation is the process of breaking up the internet into smaller, independent networks. It can be caused by a variety of factors, including government impulse for “digital sovereignty,” commercial competition, and technical incompatibility.

Whatever the impetus, internet fragmentation restricts the flow of news and information and places barriers on cross-border transfers of user data, and in practice centralizes state control over internet governance and infrastructure.¹ It also restricts access to information and knowledge which in turn also limits the exercise of socio-economic rights and political and civil rights online. For example, internet fragmentation can expose marginalized groups to potential harm by limiting access to critical information needed to combat institutionalized discrimination, creating barriers to participating in the global digital economy, and exacerbating vulnerabilities to surveillance, censorship, and discrimination. It can also aggravate discrimination and harassment of groups based on their intersectional identities, such as ethnicity, race, religion, gender/sexuality, caste, or social class by enabling governments or other actors to more easily target and isolate specific groups.

Key Principles

- An open, interoperable global internet is a fundamental tool for exercising human rights
- Multistakeholder governance is essential to avoid internet fragmentation

Recommendations

Governments:

- Endorse and meaningfully engage in multistakeholder internet governance processes at the international, regional, and national level
- Avoid laws, policies, and government regulations that would lead to internet fragmentation
- Invest in capacity building of government agencies to enable them to have a better understanding of the negative impacts of internet fragmentation, including the increased risk of cyberattacks as a fragmented internet as a patchwork of different cybersecurity standards and practices can create weaknesses attackers can exploit

¹ [Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet | Freedom House](#)

Civil society:

- Advocate for access to information offline and online without any limitation of national, regional, or international boundaries
- Support internet technical standards and norms that diminish the chance of internet fragmentation
- Advocate for a multistakeholder approach to internet governance
- Create, utilize, or share open and anonymous forms/portals for individuals to report issues that are related to internet fragmentation

Private sector:

- Develop and promote technical standards that foster global internet interoperability.
- Develop internal policies towards the promotion of international human rights standards, including access to the global internet
- Engage governments on how internet fragmentation affects business, such as impacts to cybersecurity, digital inclusion, e-commerce and electronic transactions, or trade facilitation
- Advocate within business-focused forums, such as the World Trade Organization, to ensure that an open and inclusive internet is a component of international and other international trade deals

Media:

- Improve media reporting on digital rights and internet governance including the negative impact of internet fragmentation
- Advocate for the power of a global, interoperable internet for independent media nationally and internationally at internet governance bodies

Digital Commons as a Public Good

Overview

Democracy depends on engagement and interaction, which is why the global digital commons should be protected as a public good. The internet – which is itself built upon networking protocols in the common domain – has generated a digital commons that is also a driver of knowledge exchange and innovation. This in turn, spurs social and economic progress, and is a foundation for democratic development.²

Protecting the digital commons is important for both democratic development and human development. As UN Secretary-General António Guterres has declared “it is important that all actors, including Member States, the United Nations system, the private sector and other stakeholders, promote open-source software, open data, open artificial intelligence models, open standards and open content that adhere to privacy and other applicable international and domestic laws, standards and best practices and do no harm.”³ In so doing, all stakeholders can collaborate to create a digital commons that can serve all of humanity.

Key Principles

- The digital commons must be fostered and maintained through investment in technologies and a commitment to open standards
- The digital commons should be open and accessible to all, without discrimination or exclusion based on factors such as race, gender, socio-economic status, or geography
- Collaboration is essential to the functioning of the digital commons, as it enables individuals and communities to work together to create and share digital resources

Recommendations

Governments:

- Create national policies on digital infrastructure that account for the creation and use of digital public goods
- Utilize open source software and open networking protocols
- Be transparent about the development of digital commons, and consult with multiple stakeholders during the development, deployment and review phases to prevent monopolization of power on digital commons
- Create policies that result in non-classified resources built or created using public funds to be in open licensing

² <https://policyreview.info/concepts/digital-commons>

³ https://digitalpublicgoods.net/DPGA_Strategy_2021-2026.pdf#page=13

Civil society:

- Promote and raise awareness through education and trainings
- Build initiatives on digital commons
- Advocate governments to contribute to and promote digital commons

Private sector:

- Support open standards that enable interoperability and facilitate the sharing of information across different systems and platforms
- Invest in infrastructure (broadband networks, cloud computing services, etc.) that support online collaboration and sharing

Media:

- Make use of resources in the digital public commons for reporting and dissemination of news
- Promote access to information on the digital commons

Protect data

Overview

Data protection and privacy online is fundamental to the success of democracy as it builds trust among internet users. The increased reliance of the online space has created an unprecedented amount of data that is collected, processed, stored, and shared across the internet. This is especially true since the beginning of the COVID-19 pandemic, when many social and economic activities transitioned online. With the abundance of data production and sharing, especially data that is personally identifiable, it is more important than ever to ensure that data protection and privacy are prioritized. Without these protections in place, there is an increased chance of unethical hacking, data interception, and identity theft which erodes trust in the digital space.

Key principles

- Prioritize the privacy rights of internet users
- Provide safety and security measures within technologies that help protect personally identifiable and sensitive information
- Build transparency and accountability across stakeholders including governments and businesses on how data is collected, processed, stored, shared, and disposed

Governments:

- Engage with civil society, the private sector, and independent media to develop and implement data protection policies that follow a human rights centric approach and align with international standards
- Implement a process or mechanism that ensures any collection, usage, or storage of personal data is necessary and aligns with international human rights frameworks
- Repeal laws or provisions that criminalize encryption
- Create legislation and safeguards that prohibit governments from undertaking unjustified mass surveillance

Civil Society:

- Raise awareness on data protection, and tools and practices for data protection such as data recovery systems, data backup systems, firewalls, and anti-virus software
- Review proposed data protection frameworks to ensure adherence to human rights standards
- Collaborate with technologists to inform the development of new technology that prioritizes data protection and privacy by design
- Raise awareness of best practices for digital safety and security, especially for high-risk users like journalists, human rights defenders, and activists

Private Sector:

- Develop internal policies or guidelines on data protection and privacy, and ensure data that is collected for business purposes is prioritized
- Communicate with customers/users on how their data is collected, stored, or shared. When possible, allow customers/users to opt in and agree to how their personal data will be used to maximize transparency
- Engage with civil society, independent media, and government in policy conversations focused on the development and implementation of new legislation on data privacy and protection. This engagement can help ensure that legislation on data privacy and protection not only adheres to human rights frameworks, but are feasible in terms of implementation across the business community.

Media:

- Promote investigative journalism that highlights emerging data protection issues or concerns raised by internet users
- Engage with diverse stakeholder groups, such as civil society, the private sector, and government to raise awareness on how data privacy and protection is essential for journalists and the broader media development community

Regulation of Artificial Intelligence

Overview

Artificial intelligence-based applications are influencing democratic processes at various levels including digitized civic engagement, content recommender systems, electoral content moderation, voter registration, verification and counting of votes.⁴ It is crucial to analyze the opportunities and challenges of utilizing artificial intelligence (AI) before its large-scale adoption by different stakeholders, while also being critical about the hype that goes with the term “artificial intelligence.”

Impacts of these powerful technologies require additional research, especially on how they affect democracy. This includes research and dialogue on the impact of deploying large scale AI-based technologies as well as the adoption of digital ID systems. In addition, there is a need to consider aspects of inclusion, intersectionality, as well as the environmental costs of AI.

Key Principles:

- The development and implementation of AI should not impede on digital rights essential for democratic processes
- Specific regulations for AI should be created based on the application, technology used, and sector, and incorporate public-interest auditing mechanisms
- Human review should be possible for decisions made or informed by AI systems in civil rights-related matters
- Clear accountability must be established for AI systems used in decision-making that can impact civil liberties

Recommendations

Governments:

- Invest in AI research and promote development of human-centered and human rights based AI
- Investigate and legislate to ensure that the environmental costs of AI are minimized
- Adhere to international commitments related to AI, through concrete policy, legislation, national budgets, and other executive policy instruments
- Ensure anti-discrimination and anti-bias frameworks are built into AI regulatory instruments
- Establish independent government agencies/standard setting bodies in collaboration with civil society/public interest technologists to review AI-based technologies and publish the results of such reviews

⁴ <https://analyticsdrift.com/bihar-ec-to-use-artificial-intelligence-for-automatic-vote-counting-in-panchayat-el-lections/>

- Conduct multistakeholder consultations, including work with creators of AI-based technologies, to ensure optimum regulation balancing innovation with protection of human rights and democracy
- Ensure use and development of AI used in biometrics-based Digital IDs is not undertaken without an appropriate legal framework

Civil Society:

- Advocate for the presence of diverse opinions during the stage of development of AI regulation to ensure anti-discriminatory and non-prejudiced AI-based applications
- Train policymakers and media professionals on the need to appropriately regulate AI
- Collaborate with academia to ensure that various stakeholders are aware of the risks presented by the use of AI systems in easy and accessible formats
- Campaign against the use and practice of profiling using AI-based tools to prevent government limitation on freedoms

Private sector:

- Commit to transparency about the AI tools that are developed and deployed. This includes collaborating with the media to report on new tools or features that are released
- Consider privacy and human rights implications in the design of any AI-based technology tool or platform
- Create AI-based products that can be used to bridge information gaps, especially for marginalized communities, such as people with disabilities, people of diverse genders, etc. and improve their access to public services
- Conduct regular reviews and assessments to ensure AI tools respect human rights. Key findings of impact assessments and audits of AI tools can also be published to build trust and transparency

Media:

- Conduct reporting on the development of AI, and both its social benefits and potential harms
- Examine the implications of AI on the practice of journalism to make sure that the power of AI is used in line with long-held journalistic ethics

Conclusion: The Value of Multistakeholder Democratic Digital Governance

As the online space continues to evolve at an exponential rate, there has never been a more urgent need to promote democratic digital governance. At the same time, ensuring the protection of democracy and human rights in the digital age can only be achieved through multistakeholder dialogue and collaboration, which is at the core of the recommendations and principles listed throughout this document. Continuous coordination across diverse stakeholder groups is essential to build trust, exchange ideas, and reach consensus on a wide range of issues impacting the future of democracy online. We thank the United Nations Office of the Envoy on Technology for taking these principles and recommendations into consideration.