

INPUT TO THE GLOBAL DIGITAL COMPACT

Association for Progressive Communications

Introduction

The Association for Progressive Communications (APC) firmly believes that the internet is an enabler of human rights, development and justice, including social, gender and environmental justice.

The World Summit on the Information Society (WSIS) was the foundation of digital society global policy. It articulated key values that, still today, are key for the discussion of digital cooperation, including freedom, equality, solidarity, tolerance, shared responsibility, and respect for nature. The Global Digital Compact (GDC), along with the WSIS+20 process, is an opportunity to reinterpret the WSIS vision to respond to the constantly changing digital society that we live in today. There are unquestionably challenges that persist since WSIS, while many more have emerged that expose the profound vulnerability of people and groups who have been historically discriminated against and excluded because of intersecting and multiple forms of systemic and structural inequality and injustice.

To overcome digital inclusion and achieve social justice, we must broaden the focus beyond access to connectivity infrastructure and enable political, regulatory, technical, technological and financial conditions to increase individual and collective autonomy, agency and choice in how people connect to digital technology and spaces, as well as how they use, shape, inform or create them once they are connected. There is no social justice without gender and environmental justice. Our digital future should be one in which women and people of diverse sexualities and genders are able to access and enjoy a free and open internet to exercise agency and autonomy, build collective power, strengthen movements, and transform power relations. Human rights need to be at the centre of the development, deployment, utilisation and regulation of the internet and digital technologies. The accelerated digitalisation of all aspects of life cannot be dissociated from the need to use the internet and digital technologies to adapt to and combat climate change. For this to be possible, the internet must be recognised and governed as a global public good in an inclusive, transparent, democratic and accountable manner.

The GDC could play a key role in ensuring that the lessons learned from years of multistakeholder cooperation feed into future processes of internet policy, internet governance and global digital cooperation and in setting parameters for safeguarding multistakeholderism, transparency, inclusivity, dialogue and accountability.

We believe that the GDC could help strengthen the mandate of the Internet Governance Forum (IGF), operationalise global digital cooperation and bridge the

APC believes that the IGF remains at the heart of the internet governance ecosystem. There is no
equivalent space for enabling public participation, shared learning, monitoring of progress in
achieving inclusive, human-rights based, people-centred internet and digital governance, and
discussing the positive and negative impacts of the internet and internet policies in a
multidisciplinary and multistakeholder setting. More about the IGF here:
https://www.intgovforum.org/en

gap between deliberative spaces and decision-making processes. It can also contribute to identifying the global and specific responses that differential contexts require in order to avoid perpetuating structural disadvantages, while acknowledging that the challenges we face today affect people in many different ways.

The GDC should also recall and reaffirm the human rights standards that already apply to the digital context and which offer a clear and binding framework for digital cooperation and internet governance.

In this context, APC is pleased to make a contribution to the consultation on the Global Digital Compact.

Inputs to the Global Digital Compact

As a feminist organisation that works at the intersection of human rights and digital technologies for human and ecosystems well-being, APC believes that human rights, a gender equality agenda and an intersectional feminist perspective must be placed at the core of each one of the themes of the Global Digital Compact.

In a separate joint submission, we outline in more detail the shared principles for an open, free and secure digital future for all with an expectation of having a Compact that has an intersectional gender perspective that takes into account the needs of women, girls and people of diverse genders and sexualities, in all their diversity. We also present in another separate joint submission³ the key principles that should quide a GDC process towards a future of digital governance for Earth justice and sustainable development, which refer to the need to respect planetary boundaries and the rights of nature in the design, production and deployment of digital technologies; and the need to ensure meaningful access to information, participation in decision making, and access to justice for environmental rights and the rights of nature.

This submission is oriented to provide consolidated and additional input to some of the themes of the Global Digital Compact with a focus on social, gender and environmental justice.

^{2. &}lt;a href="https://www.apc.org/en/node/38672">https://www.apc.org/en/node/38672

^{3.} https://www.apc.org/en/node/38673

Connect all people to the internet, including all schools

Problem statement

Digital exclusion persists despite the vaunted promise of connecting the next billion, and remains an obstacle for poor communities, especially those living in rural areas. Across the board, there is a slowdown in the growth of voice and internet users, whether one looks at mobile subscribers or internet penetration, and the usage gap identified by mobile operators is proving very difficult to close. The paradigms that served as foundations of policy and regulation for decades simply are not applicable or valid in the current state of the art of technology, nor for the needs of the billions of people in developing countries who still suffer from digital exclusion. Without affordable meaningful access, people are being left behind from the social and economic benefits of the digital society and economy and have no means to benefit from digital technologies, advocate for themselves, or fight for their rights as human beings. Without consideration of the local realities and needs, simply "connecting everyone" may have adverse effects rather than positive ones oriented to ensure social, environmental and gender justice, as well as an open, free and secure digital future.

Core principles

- Engagement and participation of communities in policy making concerning connectivity and access is a precondition for digital inclusion that contributes to human and ecological well-being.
- Regulatory frameworks must allow for the diversification of the connectivity providers ecosystem and the coexistence of different economic and organisational models for internet connectivity provision, including community networks and medium and small cooperative service providers or operators.
- Financing mechanisms for universalisation of connectivity must be designed and implemented to benefit small and community-based actors.
- Respect for the right of communities to build technical communications infrastructure, and to determine the how and why to connect at a pace that matches their realities, must be a central principle in digital inclusion strategies.
- Universalisation of connectivity cannot be disassociated from the selfprovision of electricity and more democratic and affordable access to spectrum and other public resources.

International Telecommunication Union. (2022, 16 September). Internet surge slows, leaving 2.7 billion people offline in 2022. https://www.itu.int/en/mediacentre/Pages/PR-2022-09-16-Internet-surge-slows.aspx

Key commitments/pledges/actions

International and multilateral organisations

 Redefine the financing mechanisms at all levels to unlock blended funding appropriate for community-based networks to build autonomous connectivity infrastructure.⁵

Governments

- Create enabling policy and regulatory environments for the development and sustainability of community-led networks.
- Regulate the internet connectivity providers ecosystem to ensure that private interests are aligned with the public interest, so as to ensure sustainable digital inclusion that serves as an equaliser and enabler of rights.
- Establish institutionalised bottom-up participation and multistakeholder decision-making processes that allow people and communities to exercise individual and collective agency, transform power relations and make access meaningful.
- Create simple, affordable licensing for community networks and make public funding available for them and other small-scale networks, particularly through the effective use of universal service funds. This includes supporting civic initiatives in small-scale infrastructure, providing training and capacity building for meaningful connectivity and content creation, offering tax incentives, and providing access to financing through microfinance institutions and other hybrid funding mechanisms and business models.
- Strengthen binding national, regional and global frameworks to implement a
 precautionary approach to digitalisation, and establish environmental and
 human rights impact assessments covering all stages of the life cycle of
 digital technologies, from design to extraction of resources, manufacturing,
 assembly and packaging, repairability and reusability, recycling and disposal.

Civil society

- Contribute to developing the capacities of communities, especially women and Indigenous people and other ethnic minorities, to connect themselves in ways that respond to their lived realities and experiences and cultures, while supporting public officials to reform their regulatory frameworks so that community networks are enabled, as a means of promoting inclusive and sustainable digital transformation.
- Advocate for an open, sustainable and accessible internet whose governance should be inclusive, transparent and participatory.
- Promote a rights-based, intersectional framework of standards, regulations and policies and support policy makers in finding solutions that ensure digital inclusion and social, gender and environmental justice.

^{5.} Forster, J., Matranga, B., & Nagendra, A. (2022). Financing mechanisms for locally owned internet infrastructure. https://www.apc.org/en/node/38259

Protect data

Problem statement

Companies are occupying public roles, resulting in an expansion of corporate power. The current internet is characterised by "the unilateral claiming of private human experience as free raw material for translation into behavioral data," resulting in surveillance capitalism. In the absence of policy and regulation to curtail the inherent abuses, the exploitation of personal data for private and political purposes has expanded to previously unimaginable proportions. Data collection never takes place in a gender-neutral setting and the gender dimension present is constantly overlooked. Methods used for activities that are inherently about labelling and categorising individuals are often predicated on existing binary gender norms. Systems developed by such data are exploited in ways that either perpetuate such norms or limit access and discriminate against those who do not conform. Moreover, the capitalisation and monetisation of data have proven how some companies prioritise profit over user privacy and public good.

Core principles

- Everyone has the right to the protection of the data that concerns them and to understand how that data is processed.
- No one shall be subjected to arbitrary interference of the right to the protection of data, and any limitation of this right shall be reasonable, necessary, proportionate and justifiable.
- The processing of data shall be fair, lawful and transparent, adhering to data processing principles set out in international norms and standards.
- Anonymity and encryption should be strengthened as tools that enable the
 enjoyment of human rights, and that create safe spaces and interactions for
 individuals and groups who face discrimination or marginalisation based on
 their gender, sexual orientation, gender identity or expression.
- Feminist and intersectional approaches to data protection and privacy must be adopted to give visibility to and question privileges that emerge as a result of gender, race, ethnicity, class and other social and cultural hierarchies.
- Indigenous peoples and traditional communities have the right to protect and steward the data and information collected in their territories, and have the right to free, prior and informed consent in relation to any technology project that may affect them or their territories.⁷

Laidler, J. (2019, 4 March). High tech is watching you. The Harvard Gazette. https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy

^{7.} Enshrined in the UN Declaration on the Rights of Indigenous Peoples: https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP E web.pdf

Key commitments/pledges/actions

Governments

- Define data governance frameworks and strengthen oversight and accountability mechanisms to increase scrutiny and transparency.
- Adopt comprehensive legal and regulatory frameworks that preserve privacy and regulate state-sponsored surveillance in line with the principles of necessity and proportionality.
- Immediately put in place a moratorium on the sale, transfer, export, servicing and use of spyware and other surveillance technologies until human rights safeguards are in place.⁸
- Review and strengthen policies and legal and regulatory frameworks to address gender-based violence in digital contexts, particularly privacy and data protection violations, and ensure that all responses are in compliance with international human rights obligations, avoiding criminalisation of speech or censorship of women's sexual expression.
- Proactively involve more women and people of diverse genders and sexualities in the development of digital technology regulations and policies.
 Promoting greater gender diversity among the people shaping online experiences is a shared responsibility of the state and the private sector.
- Respect and protect the rights of Indigenous peoples and traditional communities to protect and steward the data and information collected in their territories, and ensure that due diligence to prevent human rights violations includes a specific focus on the rights of Indigenous peoples and traditional communities.

Private sector

- Live up to their responsibilities under the UN Guiding Principles on Business and Human Rights to respect the human rights of all persons affected by their practices. This requires conducting due diligence to prevent human rights violations, mitigating adverse effects, and providing access to remedy for all persons who experience privacy violations, bearing in mind the different risks that may be faced on the basis of gender.
- Adopt and implement privacy by design/default, while applying a gendered analysis to mitigate gendered harms in the technical and organisational procedures of the technologies that companies create.
- Meaningfully engage women and people of diverse genders and sexualities in the design and development of policies, services and features, including by employing them as engineers and in policy teams.
- Allow for the use pseudonyms, which can help to enable the expression of diverse sexual and/or gender identities, and at the same time, help individuals

^{8.} OHCHR. (2019, 25 June). UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance

- to escape abusive partners, stalkers, repeat harassers and accounts associated with the sharing of non-consensual dissemination of intimate images.
- Work towards enabling technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, and resist requests for user data that do not comply international human rights standards.
- Embed users' consent into policies and user experience design.
- Meaningfully engage in consultation with women and people of diverse genders and sexualities, either by soliciting the input of users or by engaging women's rights and LGBTQI+ rights groups and activists, to understand the potential adverse impacts of the company's services on women and people of diverse genders and sexualities.

Apply human rights online

Problem statement

Human rights are integral to the realisation of human autonomy and to advancing social justice. While the COVID-19 pandemic raised multiple intersectional issues of digital security and privacy, freedom of expression, disinformation and access to information, and the further marginalisation of already marginalised communities who do not have internet access, the post-pandemic terrain that has emerged is complex. The civic space keeps shrinking at the same time that malicious state and non-state actors with racist and xenophobic motives are using technology to attack, threaten and harm women, minorities and migrants; suppress dissent; roll back human rights; and thwart advocacy by women's groups, people of diverse genders and sexualities, and marginalised communities. The complexity of the current scenario also includes the rapid digitalisation of services catalysed by the pandemic, the datafication of economies and societies, geopolitical shifts in power, and a rise of restrictive conservative and reactionary governments or policies in previously liberal democracies; polarisation of debate and perspective; a growing anxiety around resources like energy, water and food; hate narratives around migration; and potential disempowerment of multistakeholder voices in global and regional forums.

The landscape of human rights protection and promotion has changed and the private sector mediates many of our rights. There is a significantly empowered tech industry which benefited enormously from the pandemic through deals and alliances with governments in a geopolitical business war. While they jostle to set up their new models to harvest super-profits, it is anticipated that artificial intelligence (AI) technologies will significantly impact on the amount and type of disinformation circulated on the internet, including environmental disinformation, and contribute to the shaping of a new public sphere online where little can or will be trusted.

Core principles

- Alignment with existing international human rights law in all aspects pertaining
 to the digital sphere is a must to ensure accountability and transparency by
 states and corporations, address structural inequalities, strengthen
 democracy, mitigate the impact of the environmental crisis, and reinforce the
 enjoyment of human rights offline and online.
- All individuals of the global digital ecosystem, no matter who they are or where they live, should be able to fully enjoy equal rights to safety, freedom and dignity.⁹
- The internet must be operated, governed, and regulated on the legal and normative foundations of international human rights standards and the rule of law.
- Any solutions proposed to address challenges in the digital space must adhere to the principles of necessity and proportionality to avoid negative consequences for the exercise of human rights online.
- People are entitled to remedies to address violations of their internationally recognised human rights.

Key commitments/pledges/actions

Governments

- Adopt a human rights-based approach as the standard for the design and use
 of digital technologies in accordance with the standards of international
 human rights bodies and instruments.
- Undertake human rights impact assessments of digital technology-related policies, acknowledging the local contexts and realities of groups in conditions of vulnerability and marginalisation.
- Create robust frameworks for multistakeholder decision making and oversight when innovating technological responses to future crises and for the shaping of a free, open and secure digital future.
- Strengthen meaningful multistakeholder participation mechanisms where all
 those who are affected by digitalisation, particularly historically marginalised
 groups, have a say in internet governance and internet policies at all levels.

^{9.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. https://audri.org/digital-principles/

Accountability for discrimination and misleading content

Problem statement

Accountability and transparency on the part of platforms is lacking. Efforts at addressing harmful and misleading content and respecting human rights vary from company to company, and rules are often applied differently in different contexts and to different people. The lack of consistent industry-wide standards and the poor application of existing standards is not a new problem. What is new is that currently states are much more present among the loudest voices expressing concern about online content moderation. The fact that social media platforms are not exercising their responsibility to respect human rights, along with their reliance on business models that monetise "viral" content – which is also often content that is extremist, sensational and inaccurate or deliberately fake – should not immediately lead to calls for increased power for states. States in many cases have an even poorer record in communicating trustworthy information, protecting, promoting and respecting freedom of expression, and ensuring an open, diverse and plural online environment.

Core principles

- An open, diverse, free, interoperable internet enables freedom of expression, access to information, and a plural and diverse online environment.
- State and non-state actors must be held accountable for their content governance actions, in as much as they align with international human rights standards.
- Content moderation systems, both human-led and automated, must be aligned with international human rights standards and subject to transparency and accountability.

Key commitments/pledges/actions

International and multilateral organisations

- Carry out further research, with the participation of different stakeholders, into the potential impact of a variety of approaches to content regulation in different contexts. Country assessments using the UNESCO Internet Universality Indicators would be a good starting point.
- Facilitate discussions on how better to tackle problems rooted in the underlying business models of many social media platforms.
- Elaborate the practical steps that companies can take to implement the Social Media Council as a multistakeholder oversight mechanism, which serves the purpose of ensuring that platform policies are upholding the international human rights principles of non-discrimination and equality, and are taking into

account contextual factors, such as language, culture and power dynamics; and facilitates greater transparency and accountability. It should also review the human rights impacts of changes in the technical environment, the relation between these changes and harmful content, and the efficacy of regulatory responses in this regard.

Governments

- Embrace a governance approach that focuses on the regulation of company
 processes rather than content, and regulatory focus on technical systems and
 process and rules for these systems and processes. That is, regulations
 should focus on ensuring that companies are transparent and provide
 remedy, and that users can make choices about whether and how to use
 online forums.
- Ensure that limitations on freedom of expression meet established conditions of legality, necessity, proportionality and legitimacy, including on content deemed to advocate hatred and incite discrimination, hostility or violence.
- Repeal any law that criminalises or unduly restricts expression, online or offline.
- Refrain from establishing laws or arrangements that would require the "proactive" monitoring or filtering of content by companies. This would violate the right to privacy and amount to pre-publication censorship.

Platforms and companies

- Recognise international human rights law as the authoritative global standard for ensuring freedom of expression and privacy on their platforms, not their own private interests or the varying laws of states. Revise their internal policies and practices accordingly.
- Carry out human rights impact assessments on an ongoing basis. Human
 rights impact assessments should include all human rights that companies'
 policies may impact, beyond freedom of expression and privacy, and include
 economic, social and cultural rights, the right to be free from violence, and the
 right to participate in public life, among others. In addition, they should
 consider how their policies can strengthen, rather than undermine, due
 process.
- Ensure that, when dealing with requests from states, such requests cite specific and valid legal bases for restrictions and are issued by a valid government authority, in writing. Also disclose responses to government requests and to requests based on terms of services.
- Ensure and document transparency at all stages. Make transparency reports
 easy to understand and available in English and local languages. Disclose
 details concerning approaches to curation and provide meaningful and
 consistent transparency about enforcement of policies governing contentious
 issues, such as hate speech.
- Provide procedures that permit users to challenge content or account removals. Institute robust remedy programmes which may range from

- reinstatement of content to settlements related to reputational or other harms.
- Increase engagement and consultation with users, civil society and digital rights organisations.

Other areas: Environmental sustainability and digital technologies

Problem statement

The world is facing an unprecedented climate and environmental emergency and it is paramount to understand the ways in which digital technologies pose challenges to the environment, but also the constructive role they can play in confronting the crisis. The implementation of the GDC will inevitably be permeated by the success or the failure to mitigate the crisis. Thus, by setting global principles and identifying key commitments, the GDC can substantially contribute to addressing the complexity around "greening" digital technologies and to building the understanding of what technology developers, policy makers, technology companies and other actors can do to mitigate the crisis, monitor and assess the environmental impact of digitalisation, and shape responses at all levels. Global responses cannot be provided without considering the specificity of the realities that are most impacted by the depletion of resources, pollution and destruction of ecosystems and the way in which digital technologies are being designed, produced, used and discarded.

In order to build a free, open, inclusive and secure digital space, the collective dimension of rights¹⁰ has to be strengthened, particularly economic, social and cultural rights, with priority placed on the right to a dignified life.

The purpose of guiding the use of digital technologies to combat climate change and advance global environmental sustainability, as well as exploring and nurturing a granular understanding of the co-shared responsibilities that the different stakeholders have in the global digital cooperation ecosystem towards addressing the environmental and climate crisis, must be at the core of the GDC.

Core principles and key commitments and actions are detailed in APC's joint submission to the Global Digital Compact on Earth justice and sustainable development.¹¹

^{10.} This refers to the rights that by their nature are held by a group or by all, not by an individual. It also refer to the rights to minorities. The right to a clean environment is an example. Negative impacts on natural resources and territories resulting from the choice and use of digital technologies and the policies guiding their production, use and disposal (including extraction of raw materials and minerals), for instance, touch on the collective dimension of rights of people to have a healthy environment.

^{11.} https://www.apc.org/en/node/38673

About APC

The Association for Progressive Communications (APC) is an international networked organisation of activists and organisations, founded in 1990, dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technologies (ICTs). We work to create a just and sustainable world by harnessing the collective power of activists, organisations, excluded groups, communities and social movements, to challenge existing power structures and ensure that the internet is developed and governed as a global public good.

APC is currently composed by more than 60 organisational members and dozens of associates active in 74 countries and more than 50 staff with experience in implementing national, regional and global initiatives. This diverse and grounded community allows us to develop innovative and community-based access and connectivity solutions, advocate for a rights-based approach to internet access and governance, and build capacity in the women's movement, working in partnership with a diverse range of people and institutions.

More in www.apc.org

Contact information Valeria Betancourt valeriab@apc.org



JOINT SUBMISSION TO THE GLOBAL DIGITAL COMPACT ON EARTH JUSTICE AND SUSTAINABLE DEVELOPMENT

Introduction

This joint submission is a response to the Global Digital Compact consultation process and its expected outcome to outline shared principles for an open, free and secure digital future for all. We envision a Global Digital Compact that responds to the socio-environmental impacts of digital technologies, and adopts an intersectional and rights-based approach to the future of digital technologies. This submission is the result of a participatory consultation process hosted by the APC network and the Latin American Institute for Terraforming. This consultation process included an online survey, virtual meeting, and open drafting for input from participating organisations and individuals.

We have identified two intersecting principles towards a future of digital governance for Earth justice and sustainable development:

- 1. Respect planetary boundaries and the rights of nature in the design, production and deployment of digital technologies.
- 2. Ensure meaningful access to information, participation in decision making, and access to justice for environmental rights and the rights of nature.¹

These principles are aligned with existing international standards and commitments, and respond to the urgent need for action to achieve the Sustainable Development Goals (SDGs). Commitments made by all stakeholders to uphold these principles must adopt intersectional and rights-based approaches towards the future of digital technologies.

Summary of core principles and key commitments

Principle 1. Respect planetary boundaries and the rights of nature

Digitalisation must respect planetary boundaries and the rights of nature. Principle 15 of the Rio Declaration on Environment and Development (1992) states:

^

Putzer, A., Lambooy, T., Jeurissen, R., & Kim, E. (2022). Putting the rights of nature on the map: A
quantitative analysis of rights of nature initiatives across the world. *Journal of Maps*, 18(1), 89-96.
https://www.tandfonline.com/doi/full/10.1080/17445647.2022.2079432

In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.²

Governments must strengthen binding national, regional and global frameworks to implement a precautionary approach to digitalisation. Environmental and human rights impact assessments must be developed with the meaningful participation of impacted communities, and as part of broader processes of due diligence that cover all stages of the life cycle of digital technologies.

All stakeholders must commit to supporting local community-led initiatives to design, develop and deploy appropriate technologies according to their needs and local contexts. The need for autonomous and appropriate technologies is especially relevant in remote and isolated territories where extractive industries are threatening the rights and safety of traditional and Indigenous communities.³ Government and private sector commitments related to the design and deployment of digital technologies should support environmental stewardship and community-led connectivity initiatives that respect planetary boundaries and the rights of nature.

A circular economy approach to the design, production and deployment of digital technologies offers important guidance towards respecting planetary boundaries and the rights of nature. We believe that a circular economy approach must include anti-extractive, decolonial and feminist approaches.

Principle 2. Ensure meaningful access, participation and justice

Principle 10 of the Rio Declaration on Environment and Development (1992) states that environmental issues "are best handled with the participation of all concerned citizens, at relevant levels." It also framed three pillars for civic engagement in environmental decision making that form the basis of

^

^{2. &}lt;a href="https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompac">https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompac t/A CONF.151 26 Vol.I Declaration.pdf

^{3.} A good example is Rhizomatica's HERMES initiative. See: Romano, M. (2022, 11 August). Seeding change: Rhizomatica's high frequency radio showcases the power of communication in remote regions of the Amazon. APC. https://www.apc.org/en/blog/seeding-change-rhizomaticas-high-frequency-radio-showcases-power-communication-remote-regions

procedural environmental rights: access to information, participation in decision making, and access to redress and remedy.⁴

In 2019, a United Nations Environment Programme report on environmental rule of law stressed that:

These three pillars are not only practical mechanisms for implementing civic engagement, but access to these procedural guarantees has increasingly been acknowledged by the international community as the necessary basis for ensuring protection of both the emerging right to a clean and healthy environment and other substantive rights.⁵

The Aarhus Convention and Escazú Agreement are important binding regional agreements that require effective enforcement by governments and cooperation among all stakeholders. Digital technologies play a critical role in access to information and participation in decision making; however, this role is being increasingly undermined by the use of technology to target environmental activists and human rights defenders through surveillance, censorship and criminalisation of expression, online attacks, cyberstalking and disinformation.⁶

Article 9 of the Escazú Agreement commits all parties to "guarantee a safe and enabling environment for persons, groups and organizations that promote and defend human rights in environmental matters, so that they are able to act free from threat, restriction and insecurity." Commitments are needed from all stakeholders to respond to digital attacks that target environmental defenders, including sustainable funding for holistic and contextualised support for digital safety and security.⁸

Private companies must prioritise transparency and meaningful access to information relevant to the socio-environmental impacts of their operations and planned technology development. Asymmetry in access to data and information severely restricts robust and evidence-based responses from local communities to the socio-environmental impacts of digital development

А

^{4. &}lt;a href="https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompac">https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompac t/A CONF.151 26 Vol.I Declaration.pdf

^{5.} United Nations Environment Programme. (2019). *Environmental Rule of Law: First Global Report*. https://www.unep.org/resources/assessment/environmental-rule-law-first-global-report

Moolman, J., Kamran, H., & Smith, E. (2022). Freedom of expression and participation in digital spaces. Association for Progressive Communications. https://www.unwomen.org/sites/default/files/2022-12/EP.14 Jan%20Moolman.pdf

^{7. &}lt;a href="https://www.cepal.org/en/escazuagreement">https://www.cepal.org/en/escazuagreement

^{8.} Poetranto, I, Chan, S, & Anstis, S. (2020). On/offline: Multidimensional threats faced by environmental human rights defenders in Southeast Asia. In A. Finlay (Ed)., *Global Information Society Watch 2020: Technology, the environment and a sustainable world.* https://giswatch.org/node/6228

projects. Intellectual property rights must not supersede the right to a healthy environment.

Civil society representatives have important roles in amplifying the voices of impacted communities and excluded groups, and supporting their meaningful participation in decision making in processes of digital and internet governance. The rights of nature and of communities most affected by the socio-environmental impacts of digitalisation must be central to digital governance processes, and embedded in global norms and standards.

r

About APC

The Association for Progressive Communications (APC) is an international networked organisation of activists and organisations, founded in 1990, dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technologies (ICTs). We work to create a just and sustainable world by harnessing the collective power of activists, organisations, excluded groups, communities and social movements, to challenge existing power structures and ensure that the internet is developed and governed as a global public good.

More at https://www.apc.org

Contact information:

APC: shawna finnegan, shawna@apc.org



JOINT SUBMISSION TO THE GLOBAL DIGITAL COMPACT ON GENDER

INTRODUCTION

This joint submission is a response to the Global Digital Compact (GDC) consultation process and its expected outcome to outline shared principles for an open, free and secure digital future for all, with an expectation of having a Compact that has an intersectional gender perspective that takes into account the needs of women and girls, in all their diversity. This submission is one of the outcomes from a Global Digital Compact consultation that was held during the 67th session of the Commission on the Status of Women (CSW67) in New York on 14 March 2023 under the organisation of the Association for Progressive Communications and UNFPA. The consultation included the participation of organisations such as Access Now, Web Foundation, Alliance for Universal Digital Rights, Digital Rights Foundation, Resurj, KICTANet, Body and Data, Numun Fund, Amaranta NGO, Global Digital Inclusion Partnership, Women at the Table, WO=MEN, CEJIL, Multitudes, Amnesty Tech, Foundation for Media Alternatives and Point of View, among others.

As organisations that defend and protect the rights of women and people of diverse genders and sexualities, we believe that it is imperative to place the gender equality agenda at the heart of the Global Digital Compact as the Generation Equality Forum's Action Coalition on Innovation and Technology for Gender Equality has urged. In order to do so, human rights must be placed at the centre of each one of the themes both in the offline and the online world. The GDC must be based on binding, universal standards that adopt a human rights-based approach and must also recognise the differentiated impact that information and communications technologies (ICTs) have on women, girls and people of diverse genders and sexualities. We dream of a future in which all individuals of the global digital ecosystem, no matter who they are or where they live, can enjoy equal rights to safety, freedom and dignity.² This means equal and absolute protection from persecution, discrimination, abuse and surveillance; equal access to information, opportunity and community; and equal respect for privacy, identity, self-expression and self-determination.³ The core principles of the GDC of openness, freedom and security must be infused with an intersectional feminist perspective to ensure that the ongoing digital transformation of our economies and societies can usher in a genderjust world that is affirming to all individuals and their path to self-actualisation.⁴

In order to do so, the UN Global Digital Compact must:

 Recognise that there is a historically unequal power relation between men and women and, therefore, women and people of diverse genders and sexualities face a recurrent systemic gender-based discrimination.

Gurumurthy, A., & Chami, N. (2019). Charter of Feminist Demands from the Global South. Friedrich-Ebert-Stiftung. https://www.fes.de/public/FES/Newsletter-Bilder IEZ/GePol/MailingsDoc/charter-of-feminist-demandsfrom-the-global-south.pdf

^{2.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. https://audri.org/digital-principles

Ibid

^{4.} Gurumurthy, A., & Chami, N. (2019). Op. cit.

- Tackle the systemic and structural injustices in the digital society and economy stemming from the unbridled power and market excesses of the transnational platform business model.⁵
- Be grounded in values, actions and institutions resolutely committed to a gender-transformative digital paradigm that advances the rights, dignity and agency of all people in all their diversity.⁶
- Be founded on a binding human rights framework for a gender-just digital society and economy with concrete commitments for actions by state parties and transnational corporations to advance human rights of women and trans and gender-diverse persons, especially those in the Global Majority.⁷

The feminist internet that we wish to create works towards empowering more women and people of diverse genders and sexualities to fully enjoy their rights, engage in pleasure and play, and dismantle patriarchy. It integrates their realities, contexts and specificities, including age, disabilities, sexualities, gender identities and expressions, socioeconomic locations, political and religious beliefs, ethnic origins and racial markers.⁸

HUMAN RIGHTS ONLINE

Core principles

Article 1 of the UN Declaration of Human Rights states that "all human beings are born free and equal in dignity and rights." This means that the rights of all people, regardless of gender, are equal, and every person must be respected, protected, and provided with an opportunity to fulfil their interests and realise their human rights. The full realisation of human potential requires universal rights to education, to freedom of expression and information, to freedom of peaceful assembly and association including the freedom to protest and organise, as well as to full participation in and enjoyment of economic, social, cultural, civil and political life. Moreover, everyone is entitled to equal protection from all forms of discrimination, including, but not limited to, discrimination on the grounds of sex (including grounds related to pregnancy, childbirth, gender identity, intersex status and sexual orientation), race, ethnicity, colour, social or economic class, caste, disability, religion, language, political opinion, national origin, descent, veteran status, genetic information, marital status and age. 11

^{5.} Ibid.

^{6.} Ibid.

^{7.} Ibid.

^{8.} Association for Progressive Communications (APC) Feminist Principles of the Internet. https://feministinternet.org

^{9.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

^{10.} Ibid.

^{11.} Ibid.

Self-determination

The right to self-determination refers to our ability to fully exercise our agency in choosing our own destiny, including through freely determining our political status and pursuing our economic, social and cultural development. Everyone, including women, girls, trans persons, and people of diverse genders and sexualities, should be able to safely exercise self-determination in the digital age. ¹² Everyone must have the right to the complete and up-to-date representation of their identity on the internet. ¹³

Freedom of expression

Article 19 of the Universal Declaration of Human Rights establishes that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Communities and individuals who face discrimination and structural inequalities as a result of intersecting systems of oppression (sexism, racism, classism, casteism, ableism, compulsory heterosexuality, etc.) have found in the internet a critical mobilising and influencing tool to ensure state accountability and support civic action and organisation, providing possibilities for connection and solidarity across geographical boundaries to make struggles visible because of the freedom of expression. The right to freedom of expression and association as well as to protest and organise also underpins the freedom to seek, receive and impart information, and to associate freely for social, political, cultural or other purposes. It is also related to the rights to freedom of thought, conscience and religion. The religion.

Freedom of expression includes the right of sexual expression, the right to privacy and access to positive information about sex, gender and sexuality, including sexual and reproductive health rights and abortion, as part of the right to healthy emotional and sexual development.¹⁷ Feminist, queer and trans expression and visibility should not be controlled, surveilled or restricted on the internet through technology, legislation or violence. Moral policing, censorship and hierarchisation of citizenship and rights must be condemned.¹⁸

Anonymity

Everyone has the right to encryption and online anonymity. The right to be anonymous must be defended and all attempts to restrict anonymity online must be

^{12.} Ibid.

^{13.} Ibid.

^{14.} Ibid.

^{15.} Moolman, J., Kamran, H., & Smith, E. (2022). Freedom of expression and participation in digital spaces. Association for Progressive Communications. https://www.unwomen.org/sites/default/files/2022-12/EP.14 Jan%20Moolman.pdf

^{16.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit..

^{17.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

^{18.} Ibid.

rejected. Anonymity enables freedom of expression online, particularly when it comes to breaking taboos of sexuality and heteronormativity, experimenting with gender identities and expression, and enabling safety for women and people of diverse genders and sexualities affected by discrimination.¹⁹

Key commitments/pledges/actions

For governments, the private sector, civil society and other relevant stakeholders:

- Implement policies, measures and initiatives that are grounded in a human rights-based approach and that recognise, promote, protect and fulfil the rights of structurally excluded groups, including women and girls, such as women with disabilities, Black women, Indigenous women, women of colour, young women, migrant women, lesbian and bisexual women, trans women and gender-diverse people, women from oppressed castes and classes, and women from religious minority groups, as well as human rights defenders and sex workers of all genders.²⁰
- Recognise and respect the personal autonomy of people and their right to self-determination over their body, life, work, identity and sexuality.²¹
- When addressing human rights online, commit to taking an inclusive approach that goes beyond binary understandings of gender to include nonbinary, gender non-conforming, trans and intersex people.²²
- Adopt an intersectional approach when interpreting human rights that considers gender alongside race, class, caste, ethnicity, sexual orientation, religion, (dis)ability and any other relevant factor, so as to address any gendered discrimination and inequality.²³

For governments:

- States must respect, protect and promote women's human rights and those
 of LGBTQI+ persons, undertaking legal, institutional, policy and programming
 measures appropriate to the digital transformation. Robust regulation to
 prevent violation of their human rights in corporate controlled global data
 value chains is of critical importance.²⁴
- States should include in their legislation the language adopted in the 2022 Human Rights Council resolution A/HRC/50/L.11, which, among other things, calls on states:
 - to protect, respect and ensure women, girls, and LGBTQI+ persons'
 full enjoyment of the right to freedom of expression online and offline

^{19.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

^{20.} Count Me In! (n/d). Counting Sex Workers in Feminist Foreign Policies. https://cmiconsortium.org/publications/factsheet-counting-sex-workers-in-the-feminist-foreign-policies

^{21.} Ibid.

^{22.} Ibid.

^{23.} Ibid.

^{24.} Ibid.

- without discrimination and to counter all threats of violence and censorship while exercising this right;
- to refrain from imposing new restrictions including through internet shutdowns and online censorship to disrupt access to information online;
- to strengthen measures to ensure that people with disabilities can enjoy the right to freedom of expression including the freedom to seek, receive and impart information and ideas through accessible and affordable formats and technologies.
- States must uphold, respect and protect the freedom of expression online of women and girls, in all their diversities, including by refraining from censoring online expression and content relating to women's and LGBTQI+ persons' sexual and reproductive health and choice.
- State actors and their allies must be held accountable with regard to
 engaging in shutting down, restricting or over-regulating public access to the
 internet and internet-based spaces and tools, and for using existing and new
 laws aimed at digital technologies, digital security, etc. to regulate, curtail and
 control people's rights to freedom of expression, association and assembly
 online or on-ground.
- States must end the criminalisation of activists, journalists, women human rights defenders (WHRDs) and movement-actors through repealing unjust laws, policies and practices which relate to digital spaces and technologies; this must also include ending the criminalisation of young people for their activities online, e.g. through "child protection online" laws and policies, especially ending the criminalisation of young people's sexuality.
- In accordance with the prohibition on discrimination, surveillance technology should not be used to target individuals or members of a group solely based on race, colour, gender, ethnicity, Indigeneity, language, religion, age, national origin, disability, genetic information, social origin, sexual orientation, political opinion, or any other classification protected by law or on other grounds inconsistent with applicable domestic law or international obligations and commitments.²⁵

DIGITAL INCLUSION AND CONNECTIVITY

Core principles

Everyone has the right to participate in the digital realm and to access, regardless of their geographical location, universally available, secure and good-quality internet services and digital technology at an affordable price.²⁶ Nonetheless, around 4 billion people still lack access to the internet, and it is important to acknowledge that in

^{25.} Freedom Online Coalition. (2023). Guiding Principles on Government Use of Surveillance Technologies.

https://freedomonlinecoalition.com/wp-content/uploads/2023/03/FOC Guiding Principles on Government Use of Surveillance Technologies.pdf

^{26.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

many contexts, internet access is gendered. Women's and girls' ability to gain meaningful internet access is influenced by factors including location, economic power, age, gender and gender expression, racial or ethnic origin, caste, social and cultural norms, and education, among other things.²⁷

Moreover, the digital gender divide is not just an access gap; it is a democratic deficit that thwarts meaningful participation of queer and trans persons and women and girls in all their diversity in the digital transformation. The digital gender gap intersects with the other gaps and inequalities that women, girls and people of diverse genders and sexualities face in social, labour, health, economic and political spheres. According to the International Telecommunication Union (ITU), there are four main categories when talking about the gender digital divide: 1) a gap in access to and use of the internet, 2) a gap in digital skills and the use of digital tools, 3) a participation gap in science, technology, engineering and math (STEM) fields, and 4) a gap in leadership in public decision-making spaces in technology and entrepreneurship.²⁹

Additionally, digital divides can deepen other divides and inequalities and exacerbate discrimination. Women and girls, such as women with disabilities, young women, migrant women, lesbian and bisexual women, trans women and gender-diverse people, those who are marginalised due to their race, ethnicity, religion or caste, racialised women, women who live in rural areas, and women who are criminalised – among others – will continue to be excluded if there is not a comprehensive plan of action which takes an intersectional lens to women's rights. This must include an integral recognition of the diversity of experiences and needs of all women and girls. ³⁰

In order to address the structural gender digital divides that we face, digital inclusion for women and girls, in all their diversity, must be thought of as more than mere access to the internet, and must also contemplate meaningful access and active use. Connecting women and girls for the sole purpose of feeding into market logic reproduces gendered exclusions and exacerbates inequality, oppression and inequity, adding to the environmental crisis as consumption continues to increase.

^{27.} Brown, D., & Pytlak, A. (2020). Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom & Association for Progressive Communications. https://www.apc.org/sites/default/files/Gender Matters Report Web A4.pdf

^{28.} Gurumurthy, A., & Chami, N. (2019). Op. cit.

^{29.} International Telecommunication Union. (2022). *Bridging the gender divide*. https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx

^{30.} Moolman, J., Kamran, H., & Smith, E. (2022). Op. cit.

Key commitments/pledges/actions

Governments must:

- Guarantee universal, acceptable, affordable, unconditional, open, meaningful and equal access to the internet for women and people of diverse genders and sexualities.³¹
- Assure meaningful access for women and gender-diverse communities that addresses the variety of forms of digital divides, such as affordability, digital skills and continuous access, as well as accessibility for people with disabilities.
- Ensure the right of women and trans and gender-diverse persons to be
 offline, i.e. ensure that the realisation of fundamental rights and access to lifesaving and affirming services is not dependent on access to the internet and
 technology.
- Enact policies prohibiting the arbitrary and deliberate slowing and/or cutting off of the internet on any grounds, including public order or national security grounds.³²
- Make sure that the regulation of digital technologies incorporates inclusive, participatory mechanisms where all relevant stakeholders are taken into account and that these mechanisms are rights-affirming and gender-just.
- Ensure that STEM curricula are holistic and include perspectives from the social sciences and humanities and that they prioritise rights-based, genderaffirmative and climate justice-centred approaches to new technologies.
- Increase participation of women and queer and trans persons in decisionmaking processes at national and international levels on internet governance, infrastructure planning and regulation, and technology development.

They also should:

- Work with the private sector to recognise that in order to bridge the digital divide, there is no one-size-fits-all solution. There are a variety of complementary access solutions that can be successful and sustainable for connecting the unconnected, such as community networks, which may propose a different logic to traditional infrastructures by bringing feminist perspectives and feminist governance modes and models which are based on the full realisation of human rights and environmental justice.
- Gather representative and gender-disaggregated data in a consistent and
 rigorous manner to reach a better understanding of the factors shaping
 women's access to and ability to benefit from meaningful internet access in
 diverse contexts. This data should not be shared, stored or used for any other
 purpose.

^{31.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

^{32.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

- Design national broadband plans or other policies to specifically overcome gender inequalities in access.
- Increase investment in public access facilities, in particular public access strategies that emphasise women's needs, and raise awareness of the value of these facilities among disenfranchised groups.
- Encourage and support women's and queer and trans persons' participation in community and municipally owned small-scale local communications infrastructure, and make licence categories available for this type of service.

Governments, the private sector, civil society and other relevant stakeholders must:

- Ensure unrestricted access to information relevant to women and queer persons, particularly information on sexual and reproductive health and rights, safe abortion, pleasure, access to justice, and LGBTQI+ issues. This includes diversity in languages, abilities, interests and contexts.³³
- Protect and promote women's and queer and trans persons' right to code, design, adapt and critically and sustainably use ICTs to reclaim technology and the internet as a platform for creativity and expression, as well as a platform to challenge the cultures of sexism and discrimination in all spaces.³⁴ In this sense, interfaces, content and applications must be designed inclusively to ensure accessibility for all, including people with physical, sensory or cognitive disabilities, people who are not literate, and people who speak minority languages. The principle of inclusive design and the use of assistive technologies must be promoted and supported to allow persons with disabilities to benefit fully and on equal terms.³⁵

INTERNET GOVERNANCE

Core principles

The internet is a transformative political space. It facilitates new forms of citizenship that enable individuals to claim, construct and express selves, genders and sexualities. This includes connecting across territories, demanding accountability and transparency, and creating opportunities for sustained feminist movement building. The internet is also the space where social norms are negotiated, performed and imposed, often in an extension of other spaces shaped by patriarchy and heteronormativity. The collective struggle for a feminist internet is one that forms part of a continuum of feminist resistance in other spaces, public and private and in between, offline and online.³⁶

35. Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

^{33.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

^{34.} Ibid.

^{36.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

The internet was created with the utopian vision of an accessible, inclusive society that everyone in the world could inhabit democratically. Nonetheless, decades later, commercial interests have taken over, and far from being a space of freedom, the internet as become rife with misogyny, violence and hate. Unchecked development of digital technologies and networks has negatively impacted women, girls and other discriminated-against groups and structurally marginalised people. Therefore, new forms of binding governance and participation need to be established for the digital realm to ensure better protection of our rights to both safety and privacy, and to provide more effective access to recourse where infringements occur. The input of governments, technology companies, human rights organisations, civil society actors, and victims/survivors is needed to uphold and expand human rights to the fullest extent possible. The input of governments are considered to uphold and expand human rights to the fullest extent possible.

Key commitments/pledges/actions

 Internet governance should be multilateral, transparent and democratic, with the full involvement of all relevant stakeholders, including governments, the private sector, civil society, and the people most negatively impacted – including women, girls, LGBTQI+ persons, and other discriminated-against groups and structurally marginalised people.³⁹

Governments, the private sector, civil society and other relevant stakeholders must:

- Make sure more feminists and people of diverse genders and sexualities are present at decision-making tables. Internet policy making must be democratised, and ownership of and power in global and local networks must be diffused.⁴⁰
- Include the voices and experiences of young people in the shaping of internet governance and in the decisions made about safety and security online in order to promote their safety, privacy and access to information.⁴¹

Moreover:

- All decision-making processes related to the governance and development of the digital space should be open and accessible at international, regional and national levels.⁴²
- International human rights standards, the rule of law, and social justice must form the legal and normative foundations upon which the internet is operated, governed and regulated.
- There must be recourse for illegal interference and violations of human rights in the digital sphere. This shall happen in a transparent and multilateral

^{37.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

^{38.} Ibid.

^{39.} Ibid.

^{40.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

^{41.} Ibid.

^{42.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

- manner based on principles of openness, inclusive participation, and accountability. 43
- States shall mandate technology companies, companies that develop digital technologies, and digital and internet service providers to adopt human rights-based approaches in the development of their content moderation policies and practices and reporting and redressal mechanisms.⁴⁴
- The internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, universality, integrity, openness, inclusion and equal opportunity for all.
- Notified bodies and national committees should meet diversity targets in relation to representation, supported by governments, and should put into place processes and funds to enable wider and heterogeneous stakeholder participation.
- States should take steps to minimise the energy consumption of the internet and digital technologies and minimise harm from the extraction of natural resources to fuel new technologies.

DIGITAL TRUST AND SECURITY

Core principles

Everyone has a right to benefit from secure, stable and resilient digital networks and technologies. As a global public resource, the internet should be a reliable and trustworthy network for everyone. Nonetheless, the security of the internet and other digital networks is often undermined by unlawful surveillance, monitoring, and interception of users' private online activity or communications, either for individual or commercial gain or to suppress political dissent. Fears about digital safety and security are disproportionately preventing women, girls, and other discriminated-against groups and marginalised people from accessing and enjoying the internet. This, in turn, is limiting their ability to realise their rights and to engage in the digital economy.

Digital trust should be built around ethics and politics of consent in the culture, design, policies and terms of service of internet platforms. Women's agency lies in their ability to make informed decisions on what aspects of their public or private lives to share online. In this sense, women also face the manifestation of the historically unequal power relations between men and women and systemic gender-based discrimination in the form of online and technology-facilitated gender-based violence. Online gender-based violence (OGBV) tends to have a disproportionate

44. Ibid.

45. Ibid.

46. Ibid.

47. Ibid.

^{43.} Ibid.

impact on women and girls and LGBTQI+ persons, due to the oppression they face in society and their vulnerability to violence, and it can also be perpetrated against individuals on the basis of sexual orientation and gender identity. OGBV is a major hindrance to women's economic and political representation and to accessing fundamental human rights, such as the rights to freedom of expression and assembly online. It restricts civic space as it causes victims of OGBV to self-censor and limit or anonymise their engagement online.

Forms of online gender-based violence that women and people of diverse genders and sexualities face include surveillance, hate speech, gendered misinformation and disinformation, online sexual exploitation and abuse which include sexual harassment, stalking and tracking, coercive control, technology-enabled sex trafficking, livestreaming sexual abuse, and deepfakes, among others.

Key commitments/pledges/actions

Governments, the private sector, civil society and other relevant stakeholders must:

- Respect, protect and fulfil the rights of women and people of diverse genders and sexualities to liberty and security online and through the use of digital technologies. These rights must not be infringed upon or used to infringe other rights, in the online environment or through digital technologies.⁴⁸
- Maintain the inviolability of digital technologies. The ICT systems and devices
 of every person, including women, girls and people of diverse genders and
 sexualities, and the freedom and confidentiality of their electronic information
 and communications are inviolable.⁴⁹
- Guarantee network security in the public interest, ensuring infrastructure integrity and protection from external attacks and in the interest of individuals.⁵⁰
- Provide responses to disinformation, misinformation and computational propaganda generated by state and non-state actors who are using and deploying digital technologies such as artificial intelligence (AI) to mislead the public and influence major political events that affect all their lives, without their knowledge or consent.

In terms of OGBV, governments, the private sector, civil society and other relevant stakeholders should:

 Work on the elaboration and development of a comprehensive definition of online gender-based violence which reflects both the continuum of violence and the common root causes as well as the particular experiences of victims/survivors made possible through the unique specificities of digital technologies.

50. Ibid.

^{48.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

^{49.} Ibid.

 Address OGBV by providing solutions that are not only policy oriented, but also include other measures like research, movement building and strengthening community and intergenerational approaches.

Governments should specifically:

- Ensure that laws regarding gender-based violence put women's rights at the centre, such as the rights to bodily autonomy, self-determination and freedom of expression including sexual expression. States should adopt measures and legislation that protect women's right to freedom from violence and offer means of swift and meaningful redress for survivors, which also takes into account their needs, without infringing on freedom of expression and the right to information, and should implement policies that facilitate reporting of online harassment. Policies and regulations on this issue should also discourage commodification of content that promotes OGBV.
- Engage in extensive consultation with women's rights and sexual rights civil
 society organisations when creating new laws or reform regarding the
 regulation of the internet to ensure synergy with other legislative
 developments responding to OGBV and to integrate a gendered awareness
 into potential measures to avoid any discriminatory effect.
- Promote training for law enforcement, judiciary and other response actors to take GBV online seriously and react swiftly, through deepening their understanding of technology and how it can facilitate and exacerbate violence, sensitising them against victim blaming and moralistic reactions, outlining protocols to request take-down and/or obtain information from internet intermediaries following due process, etc.
- Allocate adequate budgets to address OGBV, including by providing gendersensitive training for law enforcement, legal staff, victim advocates and educators as well as provide more funding and support for civil society advocacy efforts, legal aid, capacity building, mental health care, and community building, understanding they have a key role in supporting victims of GBV.
- Recognise that comprehensive sexual education and education with a
 gender perspective are vital to address structural inequalities and violence,
 which are then transferred to the digital space, making it urgent to promote
 and implement them to eradicate technology-facilitated gender-based
 violence.
- Hold digital platforms accountable with regards to OGBV. The private sector should adopt concrete measures to respond to these forms of violence.
- Set aside morality and obscenity as rationale for protecting women and other
 communities affected by injustice. These must not be the basis for any
 legislative reform or new law in matters of gender-based violence online. Any
 law must foreground rights to bodily autonomy, self-determination, freedom of
 expression and rights to participate in public debate.

The private sector, civil society and other relevant stakeholders should:

- Ensure women, girls and LGBTQI+ persons are included throughout product development, deployment and maintenance processes, with particular attention to funding, ideation and design stages, to proactively understand and mitigate end user realities.
- Build awareness of the implications of technology-facilitated GBV among users, internet service providers and social networking platforms.
- Not suppress anonymity or encryption. Survivors often need this to re-enter online spaces, to feel safe, to share their stories and to find information.
 There are other ways to find the perpetrators.
- Ensure that data privacy and security begins from the perspective of OGBV survivors and is achieved through robust end user controls, safety-by-design, and corporate and government encryption of data in transit (end-to-end encryption between devices) and at rest (while being stored).
- Ensure legal frameworks for accountability are constructed and implemented to hold companies and offenders of technology-facilitated GBV accountable for the experiences of women, girls and LGBTQI+ persons.

Finally, legislative reform and/or new legislation regarding OGBV in and of itself is not sufficient. Holistic solutions for OGBV prevention and response should include both legal and non-legal measures, such as improving access, digital literacy, the creation of enabling environments for diverse expressions, as well as clear and specific delineations of legal and illegal gender-based hate speech.

DATA PROTECTION

Core principles

Everyone has the right to the protection of the 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 of this right, 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 data processing principles set out in international norms and standards. It is also important to recognise that there is a gender dimension present in data collection, as it never takes place in a gender-neutral setting. Methods used for activities that are inherently about labelling and categorising individuals are often predicated on existing binary gender norms. Systems developed by such data can be exploited in ways that either perpetuate such norms or limit access for and discriminate against those who do not conform.

^{51.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

^{52.} Ibid.

^{53.} Brown, D., & Pytlak, A. (2020). Op. cit.

Moreover, the capitalisation and monetisation of data have proven how the private sector prioritises profit over user privacy and public good.

Additionally, past experiences have demonstrated that, when data breaches occur, they have a more severe impact on women and gender-diverse people because of historical and structural inequalities in power relations based on gender and sexuality. Women and girls, in all their diversity, are more profoundly affected by the consequences of data breaches because they may face discrimination or even prosecution as a result. These breaches impact not only their right to privacy but also their sexual and reproductive health and rights.⁵⁴

Moreover, no matter how strong the security system is, no data is 100% safe. When data is associated with GBV it becomes categorically sensitive and if accessed, it can be used to name, shame, blame and even harass or re-offend survivors. Women and people of diverse genders and sexualities are at risk when there is not enough information on how data is collected, how it is stored and for how long, and who has access to it.

As feminist organisations, we demand that the use of data for profit and to manipulate behaviour online must end. We condemn the use of surveillance to control and restrict women's bodies, speech and activism. We believe that a feminist approach to data and datafication examines the nature of data and constantly resists disembodiment of data. It is centred on the understanding that the consequences of data and datafication, both the harms and possible benefits, are embodied within the individuals and communities facing those consequences. A feminist approach seeks to understand the effects of self-surveillance or "quantified self" developments (including the use of big data) on human rights and tries to unpack discrimination in algorithmic decision making as well as introducing feminist praxis around data. It recognises the right to privacy and to full control over personal data and information online at all levels.

Key commitments/pledges/actions

Data protection frameworks must be gender-responsive. Their design and implementation must consider gendered realities of the society we live in and ensure that injustices are not replicated as we race towards digital development.

When it comes to digitised social welfare programmes, beneficiaries, including women, should not have to choose between privacy and social protection, food security, or a benefit that after all alleviates but does not eliminate poverty.

Inferences generated by big data should be limited to safeguard people's autonomy of choice and freedom. Sensitive information should not be used to the detriment of

^{54.} Ibid.

^{55.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

the person, or to infer personal information, including their religion or sexual orientation.⁵⁶

Recommendations to governments:

- Ensure the right to data privacy and give women and gender-diverse people full control over their personal data and information online at all levels.⁵⁷
- Adopt an intersectional approach to understanding and protecting the right to privacy, which recognises the specific experiences and threats to privacy experienced by women and LGBTQI+ persons.
- Enhance efforts to promote meaningful internet access, underlining the need
 to bridge any digital divides between women and men, including through
 building digital skills, as a means to contribute to protecting against privacy
 violations of women and LGBTQI+ persons in digital contexts.
- Adopt policies and legal and regulatory frameworks that provide comprehensive protection for the use and development of secure digital communications, including by promoting strong encryption and anonymityenhancing tools, products and services.
- Review and strengthen policies and legal and regulatory frameworks to address gender-based violence in digital contexts, particularly privacy violations, and ensure that all responses are in compliance with international human rights obligations, avoiding criminalisation of speech or censorship of women's sexual expression.
- Make gender a key consideration of the development and enforcement of data protection frameworks. Data protection requirements around purpose limitation, free, explicit, prior and informed consent for data processing, data minimisation, and integrity and confidentiality of data are even more critical for people who face lateral surveillance and for whom the exploitation of their data can have more severe implications for their rights to privacy, security and other fundamental rights. The right of a data subject to rectify data to ensure that is accurate, complete and kept up-to-date can have a significant impact on the rights of a transgender person, which is not typically part of debates on data protection. The risk of processing of personal data for individual profiling leading to discrimination on the grounds of sexual orientation, gender identity, gender expression and sex characteristics is only growing as digital identity programmes are becoming mandatory in many parts of the world. Such considerations must be forefronted to safeguard the rights of women and LGBTQI+ persons in the digital age.
- Proactively involve more women and LGBTQI+ persons in the design, development and regulation of digital technologies. Reversing individual and collective attitudes that perpetuate patriarchal control and abuse of personal data and violations of the right to privacy on the basis of gender requires involving more women and LGBTQI+ people in the design, development and

^{56.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

^{57.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

regulation of digital technologies. This is not simply a matter of representation; having a more diverse and inclusive range of people contributing to the design, development and regulation of the technologies will mean that questions, concerns and considerations about the implications of privacy on these individuals and groups will arise as well as solutions to safeguard their privacy (rather than overlook or dismiss such concerns). Promoting greater gender diversity among the people shaping online experiences is a shared responsibility of the state and the private sector.

Recommendations to technology companies:

- Live up to their responsibilities under the UN Guiding Principles on Business
 and Human Rights to respect the human rights of all persons affected by their
 practices. This requires conducting due diligence to prevent human rights
 violations, mitigating adverse effects, and providing access to remedy for all
 persons who experience privacy violations, bearing in mind the different risks
 that may be faced on the basis of gender.
- Adopt and implement privacy by design/default, while applying a gendered analysis. In addition to complying with data protection frameworks, technology companies should limit data collection to restrict further data processing, to prevent unnecessary access to and exploitation of data by utilising technological means and considering privacy in the design of systems. A key component of this is privacy by default, i.e. without requiring any action by the end user. As the collection and processing of data is never gender-neutral, it is necessary to acknowledge, recognise and address how products (such as the "internet of things" or IoT and smart-home devices) or apps (such as pregnancy or dating apps, or any location-tracking app) can be exploited and used to violate the rights of women and people of diverse genders and sexualities. In light of this, it is absolutely fundamental to consider gendered harms in the technical and organisational procedures of the technologies that companies create.
- Work towards enabling technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, and resist requests for user data that do not comply with international human rights standards.
- There must be accountability for "big tech" corporations for their consistent prioritisation of profit over people by infringing on the privacy of persons for commercial benefit without their knowledge and consent, and through knowingly driving polarisation by design. Strategies for accountability must highlight design over content and acknowledge that digital technology design, the motivations which drive that design, and the actors behind the platforms are accountable for the harm they cause, and not only individual pieces of content or individual users. Corporations must achieve safety and equity on their platforms without infringing on rights and freedoms.

 Strengthen systems to support data security, including confidential information collected and managed by state actors and data collected through location-based applications and platforms.

ARTIFICIAL INTELLIGENCE AND OTHER EMERGING TECHNOLOGIES

Core principles

Until now, there is not one single definition of "artificial intelligence" (AI) that is widely accepted. It refers to the theory and design of computer systems that can perform tasks requiring some degree of human "reasoning": perception, association, prediction, planning, motor control, as well as systems that can learn from applying algorithms to large amounts of data. "Artificial intelligence" is a blanket term that could refer to varying levels and kinds of big data and algorithmic innovations such as machine learning, deep learning and neural networks.

Algorithms are at the heart of AI and are very useful tools to automate decisions. Nevertheless, we are still seeing many algorithms that discriminate against women or do not take into account people of diverse genders and sexualities. This is because they are trained using biased data sets that fail to represent the diversity of contexts and people.

As feminist organisations, we demand accountability for harms caused by algorithms and AI. We do not deny the potential of AI for public benefit, but we must acknowledge that it currently replicates the inequalities and marginalisations of our world. We need to recognise that AI and emerging technologies are being designed by people and therefore, there are gender and other intersecting biases, including race biases. If we continue to allow the profit motive to shape these technologies, they will continue to contribute to injustice and perpetuate the environmental crisis we are currently facing. We want to allow ourselves to dream larger and imagine how to place AI systems in the commons, with shared governance and shared goals of a feminist economy where AI projects and tools can be assessed through values such as agency, accountability, autonomy, social justice, non-binary identities, cooperation, decentralisation, consent, diversity, decoloniality, empathy and security, among others.

Key commitments/pledges/actions

 A presumption of algorithmic bias should always be considered, to better balance the burden of proof, and to encourage the adoption of bias mitigation tools and controls.⁵⁸

^{58.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

- There should be no judicial or administrative order or decision that could significantly impact an individual based solely on the automated processing of personal and other data which has been collected to establish the profile or personality of that person.⁵⁹
- Equality-by-design principles, including human rights and gender rights impact assessments, should be incorporated into the development of any algorithmic decision-making systems or digital technologies prior to going to market, to prevent discrimination and harmful biases being amplified and/or perpetuated.⁶⁰
- Preventative measures and safeguards should be implemented to prevent unfair, biased and arbitrary decisions being made about a person, and there should be meaningful transparency around the criteria used for decision making.⁶¹
- Al and machine learning should be trained on thick data (and not big data) for diagnostics and analysis, rather than for prediction models and drawing deterministic correlations. This will help build towards greater accountability and responsibility.
- When discussing regulation and governance of AI and emerging technologies, there must be transparency, explainability, accountability and a clear demarcation of no-go areas.
- Algorithmic auditing should be promoted in order to look at the inputs and outputs of the code of an algorithm to evaluate it for bias, in this case, gender bias.
- Accountability must be demanded from technology corporations who are building and selling artificial intelligence and automotive technologies, for purposes of state and non-state deployment, to ensure the development and ethical deployment of trustworthy AI as a public good, not as a way to erode democracy, rights, and labour standards and to further entrench discrimination. Accountability must be sought for the actors behind the development, sale, purchase and deployment of AI in anti-gender and antidemocracy campaigns.

GLOBAL DIGITAL COMMONS

Core principles

Capitalist logic drives technology towards further privatisation, profit and corporate control. Alternative forms of economic power that are grounded in principles of cooperation, solidarity, the commons, environmental sustainability and openness must be created and promoted. 62

60. Ibid.

^{59.} Ibid.

^{61.} Ibid.

^{62.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

We need to build a feminist digital economics that looks at the impact of the digital economy through a feminist lens. This includes a whole range of issues, from the infrastructure of the internet and what we are doing online that might not be thought of as work, to the ecological impacts of internet use and fresh perspectives on women's tech entrepreneurship. ⁶³

Key commitments/pledges/actions

- Governments, companies, civil society and other stakeholders should commit
 to create and experiment with technology, including digital safety and
 security, and using free/libre and open source software (FLOSS), tools and
 platforms. Promoting, disseminating and sharing knowledge about the use of
 FLOSS should be a common practice.⁶⁴
- It is not enough to talk about women's digital rights. We need a feminist
 economics to tackle inter-class and inter-country structures of inequality in
 the emerging data and AI paradigm.⁶⁵
- Digital technologies and architecture must be based on binding, open standards that ensure inclusion and equal opportunity for all. Content created and shared through the internet or digital networks should be moderated based on human rights principles.⁶⁶

LINGUISTIC AND CULTURAL DIVERSITY

Core principles

Everyone has a right to use any language of their choice to create and share digital information. ⁶⁷ Linguistic and cultural diversity enriches the development of society. All individuals and communities have the right to use their own language, or any language of their choice, to create, share and engage with information and knowledge without being exposed to harm. ⁶⁸

As more people shift their lives online, the lack of linguistic and cultural diversity in digital spaces is becoming increasingly apparent. Minority languages are often excluded from digital contexts in favour of Eurocentric languages such as English. Meanwhile, software and applications are overwhelmingly developed by the so-called majority, resulting in the limited moderation of online content in other languages and the subsequent exposure of users of those languages to online harm.

^{63.} Faith, B. (2018, 31 January). Why we need a "feminist digital economics". *GenderlT.org*. https://genderit.org/feminist-talk/why-we-need-%E2%80%98feminist-digital-economics%E2%80%99

^{64.} Association for Progressive Communications (APC) Feminist Principles of the Internet. Op. cit.

^{65.} Ibid.

^{66.} Alliance for Universal Digital Rights (AUDRi) Digital Principles. Op. cit.

^{67.} Ibid.

^{68.} Ibid.

It is crucial that the erasure of the language and cultures of all women and people of diverse genders and sexualities in the real world is not replicated in the digital realm.⁶⁹

Key commitments/pledges/actions

We need to rethink together the governance model of language infrastructures and advance towards a more fair, community-based and distributed set of governance practices. We need to enable and empower language communities to be at the core of the design of the technologies.

ENVIRONMENTAL JUSTICE

Core principles

Without regulation, the inevitable environmental impact of the construction and maintenance of digital infrastructure, and of the extraction of natural resources for use in digital technologies, are disproportionately felt by women, girls and Indigenous communities. A new regulatory framework is required to provide clarity and guidance on the expected behaviour and liability of digital technology companies. It is imperative that this framework is rooted in a feminist, intersectional analysis and developed alongside women, girls, and other discriminated-against groups and marginalised people to ensure their needs are met, instead of codifying inequality into best practice and regulatory conformity.⁷⁰