
**AFRICAN
DECLARATION**
on Internet
Rights and Freedoms



This document was prepared by members of the African Declaration group, a Pan-African initiative to promote human rights standards and principles of openness in Internet policy formulation and implementation on the continent.

For more information visit the African Declaration website africaninternetrights.org or contact a member of the African Declaration secretariat (Association for Progressive Communications, Global Partners Digital, Media Rights Agenda, Media Foundation for West Africa)

This work is provided under the Creative Commons Attribution-Non-Commercial-ShareAlike 2.5 licence. You are free to copy, distribute and display this work and to make derivative works, provided you:

- 1) give credit to The African Declaration on Internet Rights and Freedoms;
- 2) do not use this work for commercial purposes;
- 3) distribute any works derived from this publication under a licence identical to this one.

To access the full legal text of this licence, please visit:
<https://creativecommons.org/licenses/by-nc-sa/2.5/legalcode>
November 2015

INTRODUCTION

A fundamental challenge in need of urgent resolution in the digital age is how to protect human rights and freedoms on the Internet, and the African continent is no exception. The African Declaration on Internet Rights and Freedoms was developed in response to this challenge.

Access to the Internet is increasing rapidly across the African continent, with millions of individuals getting online and engaging on a wide range of issues on social media and in other digital platforms –including political matters, governance, and social and economic development, among others.

As in other parts of the world, many African countries are beginning to adopt policies, regulations or laws to regulate and, in some cases, control the Internet. In effect, many African countries are transitioning from a low regulatory Internet environment to what is fast becoming a heavily regulated environment.

Often, these laws and regulations not only fail to protect human rights but violate established human rights norms and principles without adequate safeguards.

It is therefore clear that many governments in Africa lack both the technical and legal resources to legislate appropriately and the political will to provide comprehensive protection to human rights in context of the Internet and digital technologies.

Much of the effort to regulate the Internet and online activities appears to replicate some practices from other countries which do not protect and promote human rights in relation to the Internet and digital technologies. The tendency has been for many African governments to take problematic laws from other countries or other regions and apply them with few or no changes. Invariably, the contexts and local conditions in the countries where such laws have been adopted are very different from those where the laws were originally developed.

In addition, the policy and legislative processes in most African countries lack meaningful mechanisms for inclusive participation, with the result that many critical stakeholders, particularly from civil society, are frequently excluded.

The consequence has been the adoption of instruments which tend to invade privacy, repress freedom of expression online and violate other rights, such as

the right to a fair hearing in a court of law. An analysis of these instruments shows that they often impose sanctions to punish certain types of behaviour without the requirement for due process.

Although there is a legitimate desire by governments to curb criminal activities online, particularly financial crimes and terrorist activities, there are also clear instances where the pursuit of these apparently legitimate objectives has been used as a pretext to introduce provisions to curtail criticism of governments.

The African Declaration on Internet Rights and Freedoms therefore seeks to promote human rights standards and principles of openness in Internet policy formulation and implementation on the continent.

The Declaration was motivated by the need to develop and agree on a set of principles which would inform, and hopefully inspire, policy and legislative processes on Internet rights, freedoms and governance in Africa. The principles are expected to have broad application at national, sub-regional and regional levels. In this way, the Declaration aims to cultivate an Internet environment that conforms to established human rights standards and can best meet Africa's social and economic development needs and goals.

CONTENTS

Preamble	7
Key Principles	9
1. Openness	9
2. Internet Access and Affordability	9
3. Freedom of Expression	9
4. Right to Information	9
5. Freedom of Assembly and Association and The Internet	10
6. Cultural and Linguistic Diversity	10
7. Right to Development and Access to Knowledge	10
8. Privacy and Personal Data Protection	10
9. Security, Stability and Resilience of the Internet	10
10. Marginalised Groups and Groups at Risk	11
11. Right to Due Process	11
12. Democratic Multistakeholder Internet Governance	11
13. Gender Equality	11
Application Of Principles	12
Openness	12
Internet Access And Affordability	12
Freedom of Expression	13
Right to Information	14
Freedom of Assembly and Association and the Internet	15
Cultural and Linguistic Diversity	15
Right to Development and Access to Knowledge	16
Privacy and Personal Data Protection	16
Security, Stability and Resilience of the Internet	17
Marginalised Groups and Groups at Risk	18
Due Process	18
Democratic Multistakeholder Internet Governance	19
Gender Equality	19
Call To Governments And All Other Stakeholders	21

PREAMBLE

Emphasising that the Internet is an enabling space and resource for the realisation of all human rights, including the right to hold opinions without interference, the right to freedom of expression and information, the right to freedom of assembly and association, the right to freedom of thought, conscience and religion, the right to be free from discrimination in all forms, the right of ethnic, religious or linguistic minorities to enjoy their own culture, to profess and practise their own religion, or to use their own language, and economic, social and cultural rights;

Emphasising that the Internet is particularly relevant to social, economic and human development in Africa;

Affirming that in order to fully benefit from its development potential, the Internet must be accessible, available and affordable for all persons in Africa;

Affirming further that the Internet is a vital tool for the realisation of the right of all people to participate freely in the governance of their country, and to enjoy equal access to public services;

Recalling that a number of regional standards are relevant to the protection of human rights on the Internet, in particular the African Charter on Human and Peoples' Rights of 1981, the Windhoek Declaration on Promoting an Independent and Pluralistic African Press of 1991, the African Charter on Broadcasting of 2001, the Declaration of Principles on Freedom of Expression in Africa of 2002, the African Platform on Access to Information Declaration of 2011, and the African Union Convention on Cyber-security and Personal Data Protection of 2014;

Acknowledging the roles being played by many African and international organisations, including the African Union Commission, the United Nations Economic Commission for Africa (UNECA), the NEPAD Planning and Coordinating Agency and UNESCO, in promoting access to and use of the Internet in Africa;

Mindful of the continuing efforts of international organisations and other stakeholders to develop principles that apply human rights to the Internet, particularly since the Joint Declaration of 2011 concerning Freedom of Expression and the Internet by the four Special Rapporteurs on Freedom of Expression: including the United Nations Human Rights Council resolution of 2012 on The promotion, protection and enjoyment of human rights on the

Internet; the UN General Assembly Resolution of 2013 on The right to privacy in the digital age; the UN Human Rights Council Resolution of 2014 on The Internet and Human Rights; the United Nations Guiding Principles on Business and Human Rights; the Johannesburg Principles on Freedom of Expression and National Security; The Right to Share Principles, The Necessary and Proportionate Principles; and the Manila Principles on Intermediary Liability;

Concerned by the continuing inequality in access to and use of the Internet, and the increasing use of the Internet by state and non-state actors as a means of violating individual rights to privacy and freedom of expression through mass surveillance and related activities;

Aware that some individuals and groups - in particular women and girls, people with disabilities, ethnic, religious and sexual minorities, and people living in rural areas – might be threatened with exclusion and marginalisation in relation to exercising their human rights in relation to the Internet and digital technologies;

Emphasising the responsibility of states to respect, protect and fulfil the human rights of all people;

Convinced that it is critical for all African stakeholders to invest in creating an enabling and empowering Internet environment that truly serves the needs of Africans through the adoption and implementation of this Declaration.

We herein declare:

KEY PRINCIPLES

1. OPENNESS

The Internet should have an open and distributed architecture, and should continue to be based on open standards and application interfaces and guarantee interoperability so as to enable a common exchange of information and knowledge. Opportunities to share ideas and information on the Internet are integral to promoting freedom of expression, media pluralism and cultural diversity. Open standards support innovation and competition, and a commitment to network neutrality promotes equal and non-discriminatory access to and exchange of information on the Internet.

2. INTERNET ACCESS AND AFFORDABILITY

Access to the Internet should be available and affordable to all persons in Africa without discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Access to the Internet plays a vital role in the full realisation of human development, and facilitates the exercise and enjoyment of a number of human rights and freedoms, including the right to freedom of expression and information, the right to education, the right to assembly and association, the right to full participation in social, cultural and political life and the right to social and economic development.

3. FREEDOM OF EXPRESSION

Everyone has the right to hold opinions without interference.

Everyone has a right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds through the Internet and digital technologies and regardless of frontiers.

The exercise of this right should not be subject to any restrictions, except those which are provided by law, pursue a legitimate aim as expressly listed under international human rights law (namely the rights or reputations of others, the protection of national security, or of public order, public health or morals) and are necessary and proportionate in pursuance of a legitimate aim.

4. RIGHT TO INFORMATION

Everyone has the right to access information on the Internet. All information, including scientific and social research, produced with the support of public funds, should be freely available to all, including on the Internet.

5. FREEDOM OF ASSEMBLY AND ASSOCIATION AND THE INTERNET

Everyone has the right to use the Internet and digital technologies in relation to freedom of assembly and association, including through social networks and platforms.

No restrictions on usage of and access to the Internet and digital technologies in relation to the right to freedom of assembly and association may be imposed unless the restriction is prescribed by law, pursues a legitimate aim as expressly listed under international human rights law (as specified in Principle 3 of this Declaration) and is necessary and proportionate in pursuance of a legitimate aim.

6. CULTURAL AND LINGUISTIC DIVERSITY

Individuals and communities have the right to use their own language or any language of their choice to create, share and disseminate information and knowledge through the Internet.

Linguistic and cultural diversity enriches the development of society. Africa's linguistic and cultural diversity, including the presence of all African and minority languages, should be protected, respected and promoted on the Internet.

7. RIGHT TO DEVELOPMENT AND ACCESS TO KNOWLEDGE

Individuals and communities have the right to development, and the Internet has a vital role to play in helping to achieve the full realisation of nationally and internationally agreed sustainable development goals. It is a vital tool for giving everyone the means to participate in development processes.

8. PRIVACY AND PERSONAL DATA PROTECTION

Everyone has the right to privacy online, including the right to the protection of personal data concerning him or her. Everyone has the right to communicate anonymously on the Internet, and to use appropriate technology to ensure secure, private and anonymous communication.

The right to privacy on the Internet should not be subject to any restrictions, except those that are provided by law, pursue a legitimate aim as expressly listed under international human rights law, (as specified in Article 3 of this Declaration) and are necessary and proportionate in pursuance of a legitimate aim.

9. SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Everyone has the right to benefit from security, stability and resilience of the

Internet. As a universal global public resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. Different stakeholders should continue to cooperate in order to ensure effectiveness in addressing risks and threats to security and stability of the Internet.

Unlawful surveillance, monitoring and interception of users' online communications by state or non-state actors fundamentally undermine the security and trustworthiness of the Internet.

10. MARGINALISED GROUPS AND GROUPS AT RISK

The rights of all people, without discrimination of any kind, to use the Internet as a vehicle for the exercise and enjoyment of their human rights, and for participation in social and cultural life, should be respected and protected.

11. RIGHT TO DUE PROCESS

Everyone has the right to due process in relation to any legal claims or violations of the law regarding the Internet.

Standards of liability, including defences in civil or criminal cases, should take into account the overall public interest in protecting both the expression and the forum in which it is made; for example, the fact that the Internet operates as a sphere for public expression and dialogue.

12. DEMOCRATIC MULTISTAKEHOLDER INTERNET GOVERNANCE

Everyone has the right to participate in the governance of the Internet. The Internet should be governed in such a way as to uphold and expand human rights to the fullest extent possible. The Internet governance framework must be open, inclusive, accountable, transparent and collaborative.

13. GENDER EQUALITY

To help ensure the elimination of all forms of discrimination on the basis of gender, women and men should have equal access to learn about, define, access, use and shape the Internet. Efforts to increase access should therefore recognise and redress existing gender inequalities, including women's under-representation in decision-making roles, especially in Internet governance.

APPLICATION OF PRINCIPLES

Realising these Principles on the Internet requires:

OPENNESS

In accordance with the principle of network neutrality, all data on the Internet must be treated in an equal and non-discriminatory manner, and shall not be charged differentially, according to user, content, site, platform, application, type of attached equipment, and modes of communication.

The architecture of the Internet is to be preserved as a vehicle for free, open, equal and non-discriminatory exchange of information, communication and culture. There should be no special privileges for, or obstacles against, the exchange of information online or any party or content on economic, social, cultural or political grounds. However, nothing in this Declaration may be interpreted as preventing affirmative action aimed at ensuring substantive equality for marginalised peoples or groups.

INTERNET ACCESS AND AFFORDABILITY

Access and affordability policies and regulations that foster universal and equal access to the Internet, including fair and transparent market regulation, universal service requirements and licensing agreements, must be adopted.

Direct support to facilitate highspeed Internet access, such as by establishing necessary infrastructure and infrastructure facilities, including access to openly licensed or unlicensed spectrum, electricity supply, community-based ICT centres, libraries, community centres, clinics and schools, is crucial to making the Internet accessible to and affordable for all.

Equally important is support for the establishment of national and regional Internet exchange points (IXPs) to rationalise and reduce the cost of Internet traffic at national, local and subregional levels. It is also essential to address the gender digital divide, with factors such as level of employment, education, poverty, literacy and geographical location resulting in African women having lower levels of access than men.

The sharing of best practices about how to improve Internet access for all sectors of society should be encouraged among African states.

These efforts should be geared towards ensuring the best possible level of Internet connectivity at affordable and reasonable costs for all, with particular initiatives for unserved and underserved areas and communities.

The cutting off or slowing down of access to the Internet, or parts of the Internet, for whole populations or segments of the public, should not be permitted on any grounds, including public order or national security grounds.

Internet intermediaries should be required to be transparent about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all stakeholders.

FREEDOM OF EXPRESSION

Content blocking, filtering, removal and other technical or legal limits on access to content constitute serious restrictions on freedom of expression and can only be justified if they strictly comply with international human rights law as reiterated in Article 3 of this Declaration. Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.

Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.

Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.

No-one should be held liable for content on the Internet of which they are not the author. To the extent that intermediaries operate self-regulatory systems, and/or make judgement calls on content and privacy issues, all such decisions should be made taking into account the need to protect expression that is legitimate under the principles provided for under international human rights standards, including the Manila Principles on Intermediary Liability. Processes developed by intermediaries should be transparent and include provisions for appeals.

States have a positive obligation to take steps to prevent violent attacks against anyone on their territory. These obligations take on a particular importance when individuals are attacked for exercising their right to freedom of expression online. States must create a favourable environment for participation in public debate by all the persons concerned, enabling them

to express their opinions and ideas without fear. When an attack takes place, states must launch an independent, speedy and effective investigation in order to bring both the perpetrators and the instigators to justice. They must also ensure that victims can obtain appropriate and holistic remedies for what they have suffered.

Journalists, media workers and other communicators who contribute to shaping public debate and public opinion on the Internet should be recognised as actors who enable the formation of opinions, ideas, decision-making and democracy. Attacks on all who engage in journalistic activities as a result of their work constitute attacks on the right to freedom of expression. In addition, guidelines for the protection of those who gather and disseminate information to the public, including journalists, women's rights and human rights defenders, should be put in place to ensure their safety. Such guidelines should be formulated with a view to harmonising legislative frameworks, practice, applicable regional and international standards, and law-enforcement processes at national level.

Actions should be initiated or intensified to implement such guidelines and best practices through appropriate efforts by states and other actors, including through regional cooperation, and the provision of technical assistance programmes and activities.

States should review and reform their legislation related to freedom of expression online and ensure this legislation fully complies with international standards. In particular, criminal defamation, sedition and speech related offences should be abolished, including their application on the Internet.

Rights of all to engage in individual or collective expression of oppositional, dissenting, reactive or responsive views, values or interests through the Internet should be respected. Everyone should have a right to use the Internet as a tool and/or platform for a protest action.

RIGHT TO INFORMATION

The Internet offers new opportunities to access information, and for governments to communicate with people, through the use of open data. Open data and new forms of online consultation can empower people to take a more active part in public affairs.

Data and information held by governments should be made publicly accessible, including being released proactively and routinely, except where legitimate grounds for restricting access comply with the rule of law, including relevant

freedom of information legislation.

Public authorities and private bodies which perform public functions, provide public services or utilise public funds have a duty to collect and maintain information on their operations and activities on behalf of their population. They also have an obligation to respect minimum standards in relation to the management of this information to ensure that it may easily be made accessible to all. States and relevant non-state actors should demonstrate good practices in the management of data. The use and re-use of government-held data and information should be available free of charge wherever practical. If not, pricing should be transparent, reasonable, the same for all users, and not designed as a barrier to the use or re-use of the data.

Copyrighted materials held by public bodies should be licensed for re-use in accordance with relevant access to information laws and licensing frameworks.

The existing obligation on public bodies to share all information produced with the support of public funds, subject only to clearly defined rules set out in law, as established by the Declaration of Principles on Freedom of Expression in Africa, shall extend to the proactive release of such information on the Internet in openly licensed, freely re-useable formats.

FREEDOM OF ASSEMBLY AND ASSOCIATION AND THE INTERNET

The Internet can augment the opportunities and capabilities of individuals and groups to form associations and to manage organisations and associations. It can increase the membership and reach of associations by allowing groups of people to communicate despite physical boundaries. It provides new tools for those organising assemblies offline, as well as the possibility of conducting assemblies and protests online.

Hence, everyone should enjoy unrestricted access to the Internet. Any shutting down or blocking of access to social networking platforms, and in fact the Internet in general, constitutes a direct interference with this right. Free and open access to the Internet must therefore be protected at all times.

CULTURAL AND LINGUISTIC DIVERSITY

The linguistic and cultural diversity which exists on the African continent must be promoted and reflected online. This requires states to put in place comprehensive policies, and allocation of resources, to support the development and use of tools to facilitate linguistic diversity on the Internet. This includes the promotion of technology and content required to access and use domain names, software, services and content in all languages and scripts.

Special attention should be given to promoting access in minority languages.

There is a need to promote free or low-cost training opportunities and methodologies and materials for minority-language speakers on using the Internet.

Diversity of content should also be preserved and promoted, including by encouraging diverse groups and communities to share their content online and through the digitisation of educational, scientific and cultural heritage.

RIGHT TO DEVELOPMENT AND ACCESS TO KNOWLEDGE

Developing media and information literacy is essential in ensuring that consumers of media products have the skills to find evaluate and engage with various types of information, including those relevant for their social, economic, cultural and political development.

Information and communication technologies should be designed, developed and implemented in a manner that contributes to sustainable human development and empowerment. Accordingly, policies should be adopted to create an environment which enables various actors to pursue initiatives in this regard.

Media and information literacy programmes should be instituted in schools and in other public institutions. Where practical, school children and other learners should have access to Internet-enabled devices. There is also a need for policies that improve girls' access to quality education and ICT, gender mainstreaming in Science, Technology, Engineering and Mathematics (STEM) policies, and family-friendly policies in STEM workplaces.

PRIVACY AND PERSONAL DATA PROTECTION

Personal data or information shall only be collected and/or processed by states and non-state actors such as access providers, mail providers, hosts and other intermediaries, in compliance with well-established data protection principles, including the following: personal data or information must be processed fairly and lawfully; personal data or information must be obtained only for one or more specified and lawful purposes; personal data or information must not be excessive in relation to the purpose or purposes for which they are processed; and personal data or information must be deleted when no longer necessary for the purposes for which it is collected.

The collection, retention, use and disclosure of personal data or information must comply with a transparent privacy policy which allows people to find

out what data or information is collected about them, to correct inaccurate information, and to protect such data or information from disclosure that they have not authorised. The public should be warned about the potential for misuse of data that they supply online. Government bodies and non-state actors collecting, retaining, processing or disclosing data have a responsibility to notify the concerned party when the personal data or information collected about them has been abused, lost or stolen.

Mass or indiscriminate surveillance of individuals or the monitoring of their communications, constitutes a disproportionate interference, and thus a violation, of the right to privacy, freedom of expression and other human rights. Mass surveillance shall be prohibited by law. The collection, interception and retention of communications data amounts to an interference with the right to privacy and freedom of expression whether or not the data is subsequently examined or used.

In order to meet the requirements of international human rights law, targeted surveillance of online communications must be governed by clear and transparent laws which, at a minimum, comply with the following basic principles: first, communications surveillance must be both targeted and based on reasonable suspicion of commission or involvement in the commission of serious crime; second, communications surveillance must be judicially authorised and individuals placed under surveillance must be notified that their communications have been monitored as soon as practicable after the conclusion of the surveillance operation; third, the application of surveillance laws must be subject to strong parliamentary oversight to prevent abuse and ensure the accountability of intelligence services and law enforcement agencies.

It should also be recognised that for the enjoyment of their right to privacy, individuals must be protected from unlawful surveillance by other individuals, private entities or institutions, including in their place of work or study and in public internet access points.

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Everyone has the right to enjoy secure connections to and on the Internet including protecting from services and protocols that threaten the security, stability and resilience of the Internet.

Security, stability and resilience of the Internet must be protected and technical attacks against information systems should be prevented. Encryption is one of the key ways in which this can be achieved.

States should recognise in their legislation and practices that encryption is a basic requirement for the protection of the confidentiality and security of information. In particular, States should promote end-to-end encryption as the basic standard for the protection of the rights to freedom of expression and privacy online, and promote the use of open source software.

At the same time, States should refrain from adopting measures requiring or promoting technical back-doors to be installed in hardware and software encryption products. They should repeal laws banning the use of encrypted products, particularly by end-users, or laws requiring government authorisation for the use of encrypted products.

Companies should also refrain from weakening technical standards and roll out the provision of services with strong end-to-end encryption.

Initiatives to improve security of the Internet and address digital security threats should involve appropriate collaboration between governments, private sector, civil society, academia and the technical community.

MARGINALISED GROUPS AND GROUPS AT RISK

States and non-state actors shall respect and protect the right of all individuals to have access to and use the Internet. Special attention should be paid to the needs of groups at risk of discrimination in the enjoyment of their human rights, including women, the elderly, young people and children; minorities, including ethnic, linguistic, sexual and religious minorities; and other marginalised groups such as indigenous people, persons with disabilities, and rural communities/people living in rural areas.

RIGHT TO DUE PROCESS

States must respect the right of every individual to equal protection under the law. This means that no one can be arbitrarily detained or punished for any action, including in relation to any legal claims or violations of the law regarding the Internet. Protection of this right requires entitlement to a fair and public hearing within a reasonable time by an independent, competent and impartial tribunal established by law. The court concerned should ensure that adequate relief is possible when dealing with a matter.

Jurisdiction in legal cases relating to Internet content should be restricted to States to which those cases have a real and substantial connection, normally because the author is established there, the content is uploaded there and/or the content is specifically directed at that State. Private parties should only be able to bring a case in a given jurisdiction where they can establish that they

have suffered substantial harm in that jurisdiction.

For content that was uploaded in substantially the same form and at the same place, limitation periods for bringing legal cases should start to run from the first time the content was uploaded and only one action for damages should be allowed to be brought in respect of that content, where appropriate by allowing for damages suffered in all jurisdictions to be recovered at one time (the ‘single publication’ rule).

DEMOCRATIC MULTISTAKEHOLDER INTERNET GOVERNANCE

It is important that multistakeholder decisions and policy formulations are improved at the national level in order to ensure the full participation of all interested parties. Independent, well-resourced, multistakeholder bodies should be established to guide Internet policy at the national level.

National Internet governance mechanisms should serve as a link between local concerns and regional and global governance mechanisms, including on the evolution of the Internet governance regime.

GENDER EQUALITY

Aside from addressing the gender digital divide (mentioned under Principle 2 and 13 of this Declaration), the creation and promotion of online content that reflects women’s voices and needs, and promotes and supports women’s rights, should be encouraged.

Processes and mechanisms that enable the full, active and equal participation of women and girls in decision making about how the Internet is shaped and governed should be developed and strengthened.

Conscious that the online environment reflects the inequality that women and girls face in wider society, the core principles underpinning the Internet – decentralisation, creativity, community and empowerment of users – should be used to achieve gender equality online. Wide-ranging efforts, including comprehensive legislation on rights to equality before the law and to non-discrimination, education, social dialogue and awareness-raising, should be the primary means to address the underlying problems of gender inequality and discrimination.

Women and girls should be empowered to act against gender inequality replicated on the Internet, including by using tools enabling collective monitoring of various forms of inequality, individualised tools that allow them to track and limit the availability of personal information about them online

(including public sources of data), and improved usability for anonymity and pseudonymity-protecting tools.

Additionally, all restrictions aimed at prohibiting gender-based hatred that constitutes an incitement to violence, discrimination or hostility ('incitement') should fully comply with the following conditions:

- Grounds for prohibiting advocacy that constitutes incitement should include gender;
- The intent to incite others to commit acts of discrimination, hostility or violence should be considered a crucial and distinguishing element of incitement;
- Legislation prohibiting incitement should include specific and clear reference to incitement to discrimination, hostility or violence with references to Article 20(2) of the ICCPR and should avoid broader or less specific language and should conform to the three-part test of legality, proportionality and necessity;
- Criminal law penalties should be limited to the most severe forms of incitement and used only as a last resort in strictly justifiable situations, when no other means appears capable of achieving the desired protection.

CALL TO GOVERNMENTS AND ALL OTHER STAKEHOLDERS

We call on all stakeholders to take action alone and in collaboration towards the realisation of the rights and principles in this Declaration, as outlined below:

All African stakeholders, including regional and sub-regional bodies, national governments, civil society organisations, media institutions, and relevant technology and Internet companies, should:

- Formally endorse this Declaration, the African Declaration on Internet Rights and Freedoms;
- Use this Declaration to develop a deeper understanding of how existing human rights apply to the Internet.

National governments in Africa, as principal duty-bearers, must respect, protect and guarantee the rights outlined in this Declaration, including by:

- Ratifying and giving effect to all relevant international and regional human rights treaties on human rights related to protection of human rights on the Internet, through incorporation into their domestic legislation or otherwise;
- Adopting clear legal, regulatory, and policy frameworks for the protection of these rights, in full compliance with international standards and best practice, and with the full and effective participation of civil society and other concerned stakeholders at all stages of their development;
- Providing sufficient safeguards against the violation of these rights and ensure that effective remedies for their violations are available;
- Ensuring that national regulators in the telecommunications and Internet sectors are well-resourced, transparent and independent in their operations.

Pan-African and African regional organisations and institutions:

- The African Commission on Human and Peoples' Rights should establish a mechanism to promote and monitor Internet rights and freedoms in Africa.
- The African Union should take the lead in creating a common African Programme of Action on Internet Governance, which will ensure that the rights of Africans on the Internet are promoted and upheld, and that African concerns are recognised in the global Internet governance regime.
- Other relevant pan-African institutions should develop programmes to support national institutions (including national human rights commissions and the judiciary) to understand and protect human rights online.
- The African Telecommunications Union should recognise and promote the access and affordability principle of this Declaration.

International organisations:

- UNESCO should integrate the Declaration into its “Priority Africa” strategies. UNESCO should promote the advancement of social and cultural rights on the Internet as well as the use of local languages and local content online. UNESCO should also develop model laws protecting online freedom of expression and privacy.
- The International Telecommunication Union should recognise and promote the Access and Affordability principle of this Declaration.

Civil society should:

- Seek to increase public awareness of the importance of the Internet in the realisation of human rights;
- Advocate for Internet rights and freedoms; monitor Internet laws and regulations; and highlight abuses, including in their reports to regional and international treaty bodies and other human rights mechanisms;
- Communicate with the Special Rapporteur on Freedom of Expression and Access to Information in Africa on measures to uphold freedom of expression in relation to the Internet;
- Encourage and monitor the participation of women and girls in all areas related to Internet development and governance.

Media organisations should:

- Popularise this Declaration and the principles outlined in it;
- Improve their own understanding of Internet issues and foster awareness about the importance of the Internet to all sectors of society, particularly among marginalised groups and disadvantaged communities.

All intermediaries should:

- Internalise and apply the “Respect, Protect and Remedy” framework to fulfil their duties to uphold human rights, including in relation to the Internet and digital technologies.
- Respect human rights to the fullest extent possible. For example, where faced with government demands which would violate human rights, companies should interpret government demands as narrowly as possible, seek clarification of the scope and legal foundation for such demands, require a court order before meeting government requests, and communicate transparently with users about risks and compliance with government demands.
- Invest in online tools, software and applications that enhance local and intercultural content exchange, and simplify the exchange of information across language barriers;
- Publish transparency reports on government requests for user data,

content removal, network disruptions, and compliance rates on a regular basis. All company policies on privacy and data protection, including data retention rates and breach notification policies, should be translated to local languages and easily accessible on the company's countrylevel website.

Technical communities should:

- Innovate and develop open source software, open data, and open educational resources relevant to African users;
- Engage actively in the multistakeholder processes that deal with human rights as well as Internet governance in Africa and provide policy inputs to Internet-related issues;
- Ensure African participation in the development of open standards.

Academic, research and training institutions in Africa should:

- Actively respect and promote the open standards of the Internet in terms of the technical architecture and design of the Internet;
- Integrate courses on Internet rights and freedoms in their curriculum;
- Promote and contribute to the development of local content, particularly content that fosters the use of the Internet by marginalised groups and communities;
- Proactively engage in the generation of scientific evidence on Internet rights and freedoms in Africa;
- Promote and participate in the reinforcement of Africa's capacity to contribute content and expertise in global, regional and national Internet development and policy forums.

