

CONTRACT FOR THE WEB



The Web was designed to bring people together and make knowledge freely available. It has changed the world for good and improved the lives of billions. Yet, many people are still unable to access its benefits and, for others, the Web comes with too many unacceptable costs.

Everyone has a role to play in safeguarding the future of the Web. The Contract for the Web was created by representatives from over 80 organizations, representing governments, companies and civil society, and sets out commitments to guide digital policy agendas. To achieve the Contract's goals, governments, companies, civil society and individuals must commit to sustained policy development, advocacy, and implementation of the Contract text.

Endorse the Contract for the Web
at contractfortheweb.org



GOVERNMENTS WILL

PRINCIPLE**01**

Ensure everyone can connect to the internet

So that anyone, no matter who they are or where they live, can participate actively online

1. By setting and tracking ambitious policy goals

- a. 1GB of mobile data costs no more than 2% of average monthly income by 2025.
- b. Access to broadband internet is available for at least 90% of citizens by 2030, and the gap towards that target is halved by 2025.
- c. At least 70% of youth over 10 years old and adults have Information and Communication Technology (ICT) skills by 2025.

2. By designing robust policy-frameworks and transparent enforcement institutions to achieve such goals, through

- a. Fiscal and Investment policies that stimulate investment in-and adoption of- connectivity solutions.
- b. Passive infrastructure sharing (towers, ducts on roads/rail/power lines), dig-once regulations and non-discriminatory and efficient management of radio spectrum to facilitate access to-and sharing of- spectrum for broadband connectivity.
- c. Open access rules on wholesale infrastructure in non-competitive areas, and access to license-exempt spectrum.
- d. Institutions with capacity to ensure compliance with laws and regulations designed to foster Internet adoption.

3. By ensuring systematically excluded populations have effective paths towards meaningful internet access

- a. Implementing national broadband policies with specific actions designed to target systematically excluded populations.
- b. Developing policies and providing funds for broadband strategies, including universal access and services definition, with effective technology neutral financing mechanisms for network development in unserved and underserved areas.
- c. Supporting the local production of content and applications, and the development of the necessary infrastructure and enabling environment for accelerating the growth of local digital businesses.
- d. Designing policies to increase internet access and digital literacy of women and other systematically excluded groups.

PRINCIPLE

02

Keep all of the internet available, all of the time

So that no one is denied their right to full internet access

1. By establishing legal and regulatory frameworks to minimize government-triggered internet disruptions, and ensure any interference is only done in ways consistent with human rights law

- a. Engaging in national and international multi-stakeholder dialogues and mechanisms to ensure the maintenance of uninterrupted internet connections and promoting a Web that is not restricted by public policy at borders.
- b. Engaging in transparent and documented coordination with private sector actors to ensure that any attempts to restrict access to the internet are necessary and rely on means that are proportionate to achieving a legitimate end, while minimizing the unintended side-effects of legitimate actions on third parties.
- c. Researching and documenting the cost of service interruptions to the national economy, business and users.

2. By creating capacity to ensure demands to remove illegal content are done in ways that are consistent with human rights law

- a. Passing appropriate national laws and regulations to ensure the effective enforcement of established international treaty rights on the human rights to freedom of expression, of peaceful association and assembly, and the freedom to access information as applied to online speech, behavior, and online information.
- b. Funding research and engaging in multi stakeholder forums aimed at developing future regulation on moderation dispute resolution mechanisms and content take-down, including with the aim of limiting the impacts of misinformation and disinformation, to ensure these are aligned with human rights standards.

- c. Developing mechanisms to ensure all government content take-down requests are grounded in law, properly documented, comply with human rights standards of legality, necessity and proportionality, include proper notification to the poster and potential audience, and are subject to appeal and judicial review.

- d. Developing mechanisms to ensure meaningful transparency for political advertising.

3. By promoting openness and competition in both internet access and content layers

- a. Supporting or establishing independent agencies with oversight, rule-making, and enforcement capacity to ensure internet access providers do not unreasonably discriminate against content, platforms, services, devices or users.
- b. Supporting effective enforcement of competition law at all layers of the network, including through the promotion of interoperability and open standards, as a means to ensure small actors and innovators have a fair chance to develop and successfully deploy content, new online businesses and new technologies.
- c. Funding research to determine the degree and character of competition and/or consolidation online, and its impact.

PRINCIPLE

03

Respect and protect people's fundamental online privacy and data rights

So everyone can use the internet freely, safely, and without fear

1. By establishing and enforcing comprehensive data protection and rights frameworks to

protect people's fundamental right to privacy in both public and private sectors, underpinned by the rule of law. These frameworks should be applicable to all personal data — provided by the user, observed or inferred — and include:

- a. An appropriate legal basis for data processing. Where the legal basis is consent, it must be meaningful, freely given, informed, specific, and unambiguous.
- b. The right of access to personal data, including to obtain a copy of all personal data undergoing processing by an entity, so long as such access does not adversely affect the rights and freedoms of other users.
- c. The right to object or withdraw from processing of personal data, including automated decision making and individual profiling, subject to explicit limits defined by law.
- d. The right to rectification of inaccurate personal data, and erasure of personal data, when not against the right of freedom of expression and information or other narrow limits defined by law.
- e. The right to data portability, applicable to the personal data provided by the user, either directly or collected through observing the users' interaction with the service or device.
- f. The right to redress through independent complaints mechanisms against public and private bodies that fail to respect people's privacy and data rights.

2. By requiring that government demands for access to private communications and data are necessary and proportionate to the aim pursued, lawful and subject to due process,

comply with international human rights norms, and do not require service providers or data processors to weaken or undermine the security of their products and services. Particularly, such demands should always be:

- a. Made under clearly defined laws subject to a competent and independent judicial authority that includes fair avenues for redress.
- b. Restricted to those cases where there is a legitimate public interest defined in law.
- c. Time-bounded, and not unduly restricted from disclosure to affected individuals and the public.

3. By supporting and monitoring privacy and online data rights in their jurisdictions, particularly:

- a. Minimizing their own data collection to what is adequate, relevant, and necessary to achieve a clearly specified public interest.
- b. Requiring providers of public services and private actors to comply with existing relevant legislation and supporting strong enforcement—including administrative penalties—by independent, skilled, empowered, and well-resourced dedicated regulators.
- c. Mandating public registers to promote transparency of data sharing and/or purchase agreements in public and private sectors for profiling purposes, as well as for significant data breaches that are of public interest, to make users aware of when and how their data could be exposed.
- d. Requiring regular data security and privacy impact assessments, providing independent and transparent oversight of the assessments and independent audits for public and private sectors, and enforcing when appropriate.

COMPANIES WILL

PRINCIPLE**04**

Make the internet affordable and accessible to everyone

So that no one is excluded from using and shaping the Web

1. By crafting policies that address the needs of systematically excluded groups

- a. Designing gender responsive and inclusive data plans targeting women and other systematically excluded groups.
- b. Supporting the development of community networks, particularly in unserved and underserved areas.
- c. Ensuring user interfaces and customer service are effective, and offered in languages and mediums that are accessible to minorities and people with disabilities, including by respecting universal acceptance principles.

2. By working towards an ever-increasing quality of service

- a. Documenting and publishing their investments and best efforts approach towards ensuring the speed, reliability and performance of their networks.
- b. Adopting network neutrality guidelines that ensure citizens enjoy an open, unrestricted and non-discriminatory Internet experience through which they can be not only consumers, but creators and innovators.
- c. Making progress towards symmetric upload/download speeds to facilitate the work of online creators and the use of interactive applications.

3. By ensuring full use of the internet by all, through a close coordination with Government and Civil Society towards

- a. Crafting corporate policies that minimize access barriers created by differences in language, location, age and ability.
- b. Ensuring that applications and services are designed with potentially excluded groups.
- c. Designing gender inclusive strategies to increase internet access and digital literacy by women and other systematically excluded groups.

PRINCIPLE

05

Respect and protect people's privacy and personal data to build online trust

So people are in control of their lives online, empowered with clear and meaningful choices around their data and privacy

1. **By giving people control over their privacy and data rights**, with clear and meaningful choices to control processes involving their privacy and data, including:
 - a. Providing clear explanations of processes affecting users' data and privacy and their purpose.
 - b. Providing control panels where users can manage their data and privacy options in a quick and easily accessible place for each user account.
 - c. Providing personal data portability, through machine-readable and reusable formats, and interoperable standards — affecting personal data provided by the user, either directly or collected through observing the users' interaction with the service or device.
2. **By supporting corporate accountability and robust privacy and data protection by design**, carrying out regular and pro-active data processing impact assessments that are made available to regulators which hold companies accountable for review and scrutiny, to understand how their products and services could better support users' privacy and data rights, and:
 - a. Minimizing data collection to what is adequate, relevant, and necessary in relation to the specified, explicit and legitimate purposes for which the data is processed, and limiting further processing of the data to what is compatible with those purposes.
 - b. Supporting independent research on how user interfaces and design patterns —including processes for obtaining consent and other relevant user controls — influence privacy outcomes, and ensuring those follow good privacy practices.
 - c. Enabling controls over how personal data is collected and used —including third-party and persistent tracking — that could be reviewed and adjusted at the user's convenience, and making those easy to locate and use.
 - d. Developing and adopting technologies that increase the privacy and security of users' data and communications.
3. **By making privacy and data rights equally available to everyone**, giving users options to access online content and use online services that protect their privacy, and:
 - a. Providing dedicated and readily available mechanisms for individuals to report adverse privacy and data protection impacts directly linked to the company's operations, products or services — which the company should address and mitigate as required by law.
 - b. Promoting innovative business models that strengthen data rights, respect privacy, and minimize data collection practices.
 - c. Providing clear and understandable privacy policies and consent forms, where the types of personal data processed are listed, and the purposes of data collection and use are explained.
 - d. Clearly and effectively communicating any updates and changes regarding privacy policies, as well as changes to products and services where the impact on individuals' privacy rights is not in line with the privacy policies in place.

PRINCIPLE

06

Develop technologies that support the best in humanity and challenge the worst

So the Web really is a public good that puts people first

1. By being accountable for their work, through regular reports, including how they are

- a. Respecting and supporting human rights, as outlined by the UN Guiding Principles on Business and Human Rights.
- b. Establishing policies designed to respect and promote the achievement of the Sustainable Development Goals, particularly those pertaining to education, gender equality, systematically excluded groups, climate, and socio-environmental justice.
- c. Assessing and addressing risks created by their technologies, including risks associated with online content (such as misinformation and disinformation), behavior, and personal well-being.

2. By engaging with all communities in an inclusive way:

- a. Establishing effective channels for consultation both during development of technologies and after their release, as a means to ensure the rights and interests of the full breadth of communities, in terms of gender, race, age, ethnicity, and other intersectionalities, are taken into account.
- b. Ensuring a diverse workforce: releasing periodic reports including metrics that show progress towards a more representative workforce.
- c. Ensuring their workforce is prepared in a holistic manner through periodic trainings that help employees understand their responsibilities toward the communities they affect, help them identify and tackle common blind spots, and reflect on the impact of their work.

3. By investing in and supporting the digital commons:

- a. Upholding and further developing open Web standards.
- b. Promoting interoperability, open-source technologies, open access, open knowledge, and open data practices and values.
- c. Ensuring that the terms of service, interfaces and channels of redress are accessible and available in local languages and properly localized, use formats that allow, encourage, and empower a diverse set of users to actively participate in and contribute to the commons, including open and free culture, science, and knowledge.

CITIZENS WILL

PRINCIPLE**07**

Be creators and collaborators on the Web

So the Web has rich and relevant content for everyone

By being active participants in shaping the Web, including content and systems made available through it, such as by

- a. Leveraging and promoting the use of open licenses to share information of public interest.
- b. Sharing best practices and guidelines to help create and develop a Web focused on the needs of citizens.
- c. Advocating for standard technology that is open and accessible to all persons, regardless of their abilities.
- d. Producing or translating content into local minority languages.

PRINCIPLE**08**

Build strong communities that respect civil discourse and human dignity

So that everyone feels safe and welcome online

By working towards a more inclusive Web:

- a. Adopting best practices on civil discourse online and educating the next generation on these matters.
- b. Committing to amplify the messages of systematically excluded groups, and standing up for them when they are being targeted or abused.
- c. Taking steps to protect their privacy and security, and that of others, by choosing products and services thoughtfully, and articulating privacy preferences accordingly.
- d. Refraining from participating in the non-consensual dissemination of intimate information that breach privacy and trust.

PRINCIPLE

09

Fight for the Web

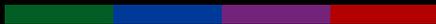
So the Web remains open and a global public resource for people everywhere, now and in the future

By being active citizens of the Web:

- a. Creating awareness amongst peers regarding threats to the open Web.
- b. Opposing the Web's weaponization by nation states or any other entity.
- c. Supporting organizations, processes and people who promote the open Web.
- d. Supporting startups and established companies that espouse the Web's future as a basic right and public good.
- e. Engaging political representatives and companies to ensure support and compliance with this Contract and support for the open Web.

ANNEX

This Annex includes links to a selection of human rights and other frameworks that relate to the Contract's substance, and a Glossary that provides references aimed at supporting the understanding of the Contract.



WORKING GROUP

A: Access

List of members: <https://contractfortheweb.org/access/>

Chairs: Lydia Carroon & Eleanor Sarpong

External Expert: Mike Jensen

PRINCIPLE 1

[Governments will] Ensure everyone can connect to the internet

So that anyone, no matter who they are or where they live, can participate actively online

CONTEXT

Internet access has become a cornerstone of human development: Offering individuals and communities access to an immense corpus of knowledge through which to develop their identities and harness a broader understanding of the world we live in. The Internet has also become a means of access to public goods and services, and given that those with limited internet access are typically the same groups who suffer from other forms of exclusion, this new form of exclusion further widens the gap between haves and have-nots that is already creating tensions in societies across the globe.

Thus, governments should adopt policies towards the provision of internet access to all persons, regardless of their status or geography, ensuring standards for reliability and security are met, whilst fostering demand for, and improving the potential benefits of connectivity. This requires smart policies and provisions to ensure not only that everyone can access the internet, but also the skills to use it effectively through technical training and digital literacy programmes.

HUMAN RIGHTS FRAMEWORK

This section includes non-exhaustive list of references to United Nations documents that provide a foundation for the interpretation of human rights in the context of the Web.

Preamble to the International Covenant on Economic, Social and Cultural Rights (ICESCR):

‘Recognizing that, in accordance with the Universal Declaration of Human Rights, the ideal of free human beings enjoying freedom from fear and want can only be achieved if conditions are created whereby everyone may enjoy his economic, social and cultural rights, as well as his civil and political rights.’

“Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States. Each State should thus develop a concrete and effective policy, in consultation with individuals from all sections of society, including the private sector and relevant Government ministries, to make the Internet widely available, accessible and affordable to all segments of population.”

- Report of the United Nations High Commissioner for Human Rights, 5 May 2017 ([A/HRC/35/9](#))

Article 19 of the Universal Declaration of Human Rights (UDHR): ‘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.’

“Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet. Access to the Internet is also necessary to promote respect for other rights, such as the rights to education, health care and work, the right to assembly and association, and the right to free elections.”

- **Joint Declaration** by UN Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 2011

“States should create a policy and legislative environment conducive to a diverse, pluralistic information environment...”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29 August 2018 ([A/73/348](#))

Article 26 of the Universal Declaration of Human Rights (UDHR): ‘Everyone has the right to education.’

“Quality education plays a decisive role in development, and therefore calls upon all States to promote digital literacy and to facilitate access to information on the Internet, which can be an important tool in facilitating the promotion of the right to education.”

- **Human Rights Council**, 1 July 2016 ([A/HRC/RES/32/13](#))

“States should include Internet literacy skills in school curricula, and support similar learning modules outside of schools. In addition to basic skills training, modules should clarify the benefits of accessing information online, and of responsibly contributing information.”

- **Frank La Rue** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011 ([A/HRC/17/27](#))

Article 27 of the Universal Declaration of Human Rights (UDHR): ‘Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.’

“Governments must respect and protect freedom of information and expression, including on the Internet to ensure the implementation of article 15 of the Covenant. With the Internet emerging as a critical platform for scientific and cultural flows and exchanges, freedom of access to it and maintaining its open architecture are important for upholding the right of people to science and culture.”

- **Farida Shaheed** - Special Rapporteur in the field of cultural rights, 14 May 2012 ([A/HRC/20/26](#))

Article 7 of the Universal Declaration of Human Rights (UDHR): ‘... All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.’

“Gender equality should be promoted in the design and implementation of ICTs and in the policy decisions and frameworks that regulate them. It is critical for all stakeholders to invest in creating an enabling and empowering ICT environment that serves the needs of women by respecting, protecting and promoting their human rights online...”

States should collect, analyse and track sex-and gender-disaggregated data on ICT access and usage in order to reach a better understanding of how digital inclusion can be achieved and how to develop informed policies.”

- **Report of the United Nations High Commissioner for Human Rights**, 5 May 2017 ([A/HRC/35/9](#))

Article 9 of the Convention on the Rights of Persons with Disabilities (CRPD): “[The States Parties to the present Convention ... have agreed:] To enable persons with disabilities to live independently and participate fully in all aspects of life, States Parties shall take appropriate measures to ensure to persons with disabilities access, on an equal basis with others,

to the physical environment, to transportation, to information and communications, including information and communications technologies and systems, and to other facilities and services open or provided to the public, both in urban and in rural areas. These measures, which shall include the identification and elimination of obstacles and barriers to accessibility...”

“Legislation should incorporate and be based on the principle of universal design, as required by the Convention (art. 4, para. 1 (f)). It should provide for the mandatory application of accessibility standards and for sanctions, including fines, for those who fail to apply them. Efforts should also be made to achieve the interoperability of goods and services, especially in the field of transport, information and communication, including the Internet and other ICT, through the promotion of internationally recognized accessibility standards.”

- **Committee on the Rights of Persons with Disabilities**, 25 November 2013 (CRPD/C/11/3)

The sections above are a selection of the many Human Rights that government officials should uphold when developing policies that affect the internet.

OTHER EXISTING FRAMEWORKS

This section includes references to frameworks that third parties have developed to further delineate rights and principles in the context of the Web. Though this list is not exhaustive, it can provide further support to those interested in understanding the Contract’s objectives.

UN Sustainable Development Goals (SDGs):

Adopted by world leaders in September 2015, the document establishes a clear link between Internet access and the achievement of all of the United Nations SDGs. It also establishes clear goals towards infrastructure roll out, such as through Target SDG 9c – “Universal and affordable access across the world’s Least Developed Countries (LDCs) by 2020.”

The Tunis Agenda for the Information Society:

A consensus statement adopted in 2005 at the World Summit on the Information Society, which set the ground for the creation of the Internet Governance Forum (IGF). It includes a clear call to action for affordable access in line C2 – “Infrastructure is central in achieving the goal of digital inclusion, enabling universal, sustainable, ubiquitous and affordable access to ICTs by all, taking into account relevant solutions already in place in developing countries and countries with economies in transition, to provide sustainable connectivity and access to remote and marginalized areas at national and regional levels.”

PRINCIPLE 4

Make the internet affordable and accessible to everyone

So that no one is excluded from using and shaping the web

CONTEXT

The availability of affordable internet access options has become vital to achieving economic, social and human development, and the exercise of basic human rights.

As such, the private sector is called to play a key role in responding to citizen’s need for service of sufficient quality and broad accessibility.

HUMAN RIGHTS FRAMEWORK

Preamble to the International Covenant on Economic, Social and Cultural Rights (ICESCR):

‘Recognizing that, in accordance with the Universal Declaration of Human Rights, the ideal of free human beings enjoying freedom from fear and want can only be achieved if conditions are created whereby everyone may enjoy his economic, social and cultural rights, as well as his civil and political rights.’

“Among the most important steps that private actors should take is the development and implementation of transparent human rights assessment procedures... Such assessments should critically review the wide range of private sector activities in which they are engaged, such as the formulation and enforcement of terms of service and community standards on users’ freedom of expression, ... including design and engineering choices, and plans for differential pricing of or access to Internet content and services...”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 11 May 2016 ([A/HRC/32/38](#))

“Public consultations and engagement should occur prior to the finalization or roll-out of a product or service, in order to ensure that they are meaningful, and should encompass engagement with civil society, human rights defenders and representatives of marginalized or underrepresented end users. The results of human rights impact assessments and public consultations should themselves be made public.”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29 August 2018 ([A/73/348](#))

Article 7 of the Universal Declaration of Human Rights (UDHR): ‘... All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.’

“Gender equality should be promoted in the design and implementation of ICTs and in the policy decisions and frameworks that regulate them. It is critical for all stakeholders to invest in creating an enabling and empowering ICT environment that serves the needs of women by respecting, protecting and promoting their human rights online.

States and business enterprises should act to prevent and combat online violence against women. They should collect comprehensive data on the extent and nature of online violence against women and conduct further research to understand and address its underlying causes and how best to combat it. Civil society should monitor this data collection to ensure it is done in an effective and gender-sensitive manner...”

- **Report of the United Nations High Commissioner for Human Rights**, 5 May 2017 ([A/HRC/35/9](#))

OTHER EXISTING FRAMEWORKS

The Guiding Principles on Business and Human Rights: Implementing the United Nations ‘Protect, Respect and Remedy’ Framework, developed in 2011 by the Special Representative of the Secretary-General, covers the issue of human rights and transnational corporations and other business enterprises from a broad perspective.

The United Nations Guidelines for Consumer Protection: States that digital goods and services must be held to the same consumer protection standards as those in the physical world. Outlines companies should offer customers a fair and equitable treatment, accurate information regarding the goods and services offered, and develop programmes and mechanisms to assist consumers to develop the knowledge and skills necessary to understand the risks and benefits associated with their products and services.

The Charter of Human Rights & Principles for the Internet: Published by the UN Internet Governance Forum (IGF) Internet Rights and Principles Coalition in 2014, the document offers guidelines to companies about how they should behave so as to respect human rights in the Internet environment, and establishes quality of service, net neutrality, digital inclusion and freedom of choice in terms of software and hardware as pillars of the right to internet access.

WORKING GROUP

B: Openness

List of members: <https://contractfortheweb.org/openness/>

Chairs: Besart Copa & Nnenna Nwakanma

External Expert: Avri Dovra

PRINCIPLE 2

Keep all of the Internet available, all of the time

So that no one is denied their right to full internet access

CONTEXT

The transformative nature of the Internet means that it is involved in many, if not most, facets of modern life. Studies have shown the disruption of Internet access is not free but rather cost dearly. Not only do Internet disruptions affect the lives and rights of citizens, they interfere with all manner of commerce. Shutdowns of the Internet have been occurring at an increasing rate. Research has shown the cost to national economies to be in the billions of dollars.

Specifically the scope of internet openness covers anything that affects the ability for anyone to freely communicate with anyone else at any time from anywhere about any subject with the bounds set by internationally agreed standards of Human Rights. Whether it is a matter of rights or of economy, disrupting the openness of the Internet has negative effects on the well being of nations.

HUMAN RIGHTS FRAMEWORK

While all of the rights defined in the Universal Declaration of Human Rights and covenants are equal and inseparable, several have particular relevance to Openness of the Internet and serve as the underpinning for the public interests of the rights holders related to their freedoms on the Internet, several have a high degree of significance to openness on the Internet.

Article 19 of the Universal Declaration of Human Rights (UDHR): '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.'

"Indeed, the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as guaranteed by Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The latter provides that: (a) Everyone shall have the right to hold opinions without interference; (b) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice; (c) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (d) for respect of the rights or reputations of others; (e) for the protection of national security or of public order (ordre public), or of public health or morals."

- **Frank La Rue** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011 ([A/HRC/17/27](#))

"In this regard, the Special Rapporteur also emphasizes that the existing international human rights standards, in particular article 19, paragraph 3, of the International Covenant on Civil and Political Rights, remain pertinent in determining the types of restrictions that are in breach of States' obligations to guarantee the right to freedom of expression."

- **Frank La Rue** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011 ([A/HRC/17/27](#))

Article 20 of the Universal Declaration of Human Rights (UDHR):

- (1) Everyone has the right to freedom of peaceful assembly and association.
- (2) No one may be compelled to belong to an association.

"[The United Nations' Human Rights Council] Calls upon all States to address security concerns on the Internet in accordance with their international human rights obligations to ensure protection of freedom of expression, freedom of association, privacy and other human rights online, including through national democratic, transparent institutions, based on the rule of law, in a way that ensures freedom and security on the Internet so that it can continue to be a vibrant force that generates economic, social and cultural development."

- **The UN Human Rights Council**, 27 June 2016 ([A/HRC/32/L.20](#))

Article 27 of the Universal Declaration of Human Rights (UDHR):

- (1) Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.
- (2) Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author.

"With the Internet emerging as a critical platform for scientific and cultural flows and exchanges, freedom of access to the Internet and maintaining its open architecture are important for upholding the right to participate in cultural life and to enjoy the benefits of scientific progress and its applications."

- **Frank La Rue** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011 ([A/HRC/17/27](#))

Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

- (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
- (3) The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
 - (a) For respect of the rights or reputations of others;
 - (b) For the protection of national security or of public order (ordre public), or of public health or morals.

With relation to these rights, several organisms, including the Special Rapporteurs, have made frequent reference to the application of these rights, as well as all other rights in the inseparable declaration of rights, to online human activity.

“Any restriction [to art. 19.3 of the ICCPR, regarding the right to freedom of expression], to be lawful, must protect only those interests enumerated in article 19 (3): the rights or reputations of others, national security or public order, or public health or morals. Restrictions designed to protect the rights of others, for instance, include ‘human rights as recognized in the Covenant and more generally in international human rights law’. Restrictions to protect rights to privacy, life, due process, association and participation in public affairs, to name a few, would be legitimate when demonstrated to meet the tests of legality and necessity.”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report, 6 April 2018 ([A/HRC/38/35](#))

“Filtering of content on the Internet, using communications ‘kill switches’ (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law.”

- **Joint Declaration** by the United Nations Organization for Security and Co-operation in Europe, the Organization of American States and the African Commission on Human and Peoples’ Rights, 4 May 2015 ([Joint Declaration on Freedom of Expression and responses to conflict situation](#))

“... blocking is not justified to pursue aims which are listed under article 19, paragraph 3, of the International Covenant on Civil and Political Rights, and blocking lists are generally kept secret, which makes it difficult to assess whether access to content is being restricted for a legitimate purpose. [E]ven where justification is provided, blocking measures constitute an unnecessary or disproportionate means to achieve the purported aim, as they are often not sufficiently targeted and render a wide range of content inaccessible beyond that which has been deemed illegal.”

- **Frank La Rue** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011 ([A/HRC/17/27](#))

“The Special Rapporteur calls upon States that currently block websites to provide lists of blocked websites and full details regarding the necessity and justification for blocking each individual website. An explanation should also be provided on the affected websites as to why they have been blocked. Any determination on what content should be blocked must be undertaken by a competent judicial authority or a body which is independent of any political, commercial, or other unwarranted influences.”

- **Frank La Rue** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011 ([A/HRC/17/27](#))

“Human rights law guarantees individuals a remedy determined by competent judicial, administrative or legislative authorities (article 2 (3) of the Covenant). Remedies must be known by and accessible to anyone who has had their rights violated; must involve prompt, thorough and impartial investigation of alleged violations; and must be capable of ending ongoing violations...”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29 August 2018 ([A/73/348](#))

“Unlike the right to form and hold opinions, the rights to express and access information and ideas may be subject to restrictions under limited circumstances (article 19 (3) of the Covenant)...In an AI-governed system, the dissemination of information and ideas is governed by opaque forces with priorities that may be at odds with an enabling environment for media diversity and independent voices. Relevantly, the Human Rights Committee has found that States should “take appropriate action ... to prevent undue media dominance or concentration by privately controlled media groups in monopolistic situations that may be harmful to a diversity of sources and views.

...States should create a policy and legislative environment conducive to a diverse, pluralistic information environment...”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29 August 2018 ([A/73/348](#))

“In order to protect against unaccountable private domination of the environment for freedom of expression, we urge the development of ...: Human rights sensitive solutions to the challenges caused by disinformation, including the growing possibility of ‘deep fakes’, in publicly accountable and targeted ways, using approaches that meet the international law standards of legality, legitimacy of objective, and necessity and proportionality.”

- **United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression**, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples’ Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, 2018 ([Joint Declaration on Media Independence and Diversity in the Digital Age](#))

OTHER EXISTING FRAMEWORKS

The Tunis Agenda for the Information Society:

A consensus statement adopted in 2005 at the World Summit on the Information Society, which set the ground for the creation of the Internet Governance Forum (IGF). While currently primarily a discussion space, there are efforts towards formalizing the outputs from the activities that take place there. The IGF, and other IGF like efforts, should be looked at with consideration of the recommendations made in The Age of Digital Interdependence report from the UN High-Level Panel on Digital Cooperation for furthering and improving the effectiveness of the current models of Internet governance and regulatory function.

UNESCO ROAM Principles: The framework promotes the embracing of four principles believed to have been core fundamental to the development of the Internet Rights based, Openness, Accessibility and Multi-stakeholder participation (ROAM), which offers a special focus on access to information and knowledge, freedom of expression, privacy and ethics. They were agreed upon by UNESCO member states in 2015, are currently being applied in diverse fields including blocking and filtering and in artificial intelligence. The value of these principles was acknowledged by the UN Secretary-General’s High Level Panel on Digital Cooperation.

WORKING GROUP

C: Privacy and Data Rights

List of members: <https://contractfortheweb.org/privacy-and-data-rights/>

Chair: Carlos Iglesias

External Expert: Matthew Rice

PRINCIPLE 3

Respect and protect people's fundamental online privacy and data rights

So everyone can use the Web freely, safely and without fear

CONTEXT

Across the world, in every culture and society there is a notion of privacy and liberty. They may be established in different forms or fall under different categories, but they do exist, underpinned by international frameworks like the Universal Declaration of Human Rights. As we move more of our lives online, the rules and customs that respect the universal and fundamental right to privacy are even more important.

We are faced with a new set of challenges in relation to our privacy and data rights in an era where the generation of data, its collection over the Web, and analytics power increases and more of the Web becomes an observed space. This includes not just the data that we provide ourselves, but the data that are generated or attributed to us through monitoring and tracking our use of the Web. There is now a pressing need for Governments to respect the privacy and data rights of individuals and communities to allow users to retain a sphere of autonomy where they can explore the Web freely without the threat of coercion, control, interference or surveillance, and for setting strong laws and policies that companies and other entities must comply with.

This principle focuses on the role of Governments in establishing frameworks for respecting, protecting and fulfilling people's right to privacy and data rights. The aim of establishing these principles and clauses is to create a world in which everyone can use the Web freely, safely and without fear.

HUMAN RIGHTS FRAMEWORK

Privacy and other data rights have their basis in pre-existing human rights frameworks. The respect and protection of these international frameworks, interpreted to reflect the digital age, provide the strongest basis from which to base the contractual principles. Reflecting that other areas of the contract provide a basis from which to understand wider rights of access to information and openness, the core rights at play in privacy and other data rights are:

Article 12 of the Universal Declaration of Human Rights (UDHR): 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

"The right to privacy must be protected by standards of confidentiality and integrity of IT-Systems, providing protection against others accessing IT-Systems without consent."

- **IGF Charter of human rights and principles for the Internet**, 2014

Article 17 of the International Covenant on Civil and Political Rights (ICCPR): 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.'

“States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons.... The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law.... In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files.”

- **Human Rights Committee**, General Comment 16, adopted on 8 April 1988

Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

- (1) Everyone shall have the right to hold opinions without interference.
- (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

“It follows that any capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to freedom of expression and association... The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful.”

- **Office of the High Commissioner of Human Rights**, 30 June 2014 (A-HRC-27-37)

OTHER EXISTING FRAMEWORKS

Beyond the core Human Rights International Legislation mentioned above (UDHR and ICCPR), we also consider the following existing frameworks:

EU General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council¹, the European Union’s (‘EU’) new General Data Protection Regulation (‘GDPR’), regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU.

APEC Cross-Border Privacy Rules System: The APEC Cross-Border Privacy Rules (CBPR) System is a government-backed data privacy certification that companies can join to demonstrate compliance with internationally-recognized data privacy protections. The CBPR System implements the APEC Privacy Framework endorsed by APEC Leaders in 2005 and updated in 2015.

International Principles on the Application of Human Rights to Communications Surveillance:

These principles are the outcome of a global consultation with civil society groups, industry, and international experts in Communications Surveillance law, policy, and technology. They seek to provide civil society groups, industry, States, and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

OECD Principles for Internet Policymaking:

The Principles for Internet Policymaking from the Organization for Economic Cooperation and Development (OECD) seek to ensure compatibility across a diverse set of laws and regulations to support the global free flow of information. The principles appeal to Governments and private actors to seek empowerment of users, strengthen consistency and effectiveness in privacy protection at a global level, and ensure transparency, fair process, and accountability.

OECD Privacy Guidelines: The OECD Privacy Guidelines articulate many of the same principles that operate under the European Union’s national data protection legislation. Doing so at an international level means the Privacy Principles have served as the basis for creating emerging privacy and data protection laws. The guidelines show how the protection of privacy and individual liberties adopted by the various countries have many common features such as limits to the collection of personal data, restricting the usage of data to conform with openly specified purposes, security safeguards and individual participation, among others.

PRINCIPLE 5

Respect and protect people's privacy, personal data, and other online data rights to build online trust

So people are in control of their lives online, empowered with clear and meaningful choices around their data and privacy

CONTEXT

The Web has become one of the principal means by which individuals exercise their right to freedom of expression and information. It provides essential tools for participation and discussions concerning political issues and issues of general interest.

Through the Web, platforms are becoming the de facto meeting points, where public discourse and debate occurs. They provide space for communities to meet, discuss, share ideas, and make change happen. They are our town halls and our cafes, our libraries and our newsagents. Moreover, the amount and granularity of personal data available today, and the increasing complexity of data processing techniques, raise serious concerns about possible negative impacts on our privacy and data rights.

With this increased centrality to our lives, platforms have direct effects on our fundamental rights. Their choices of business model, platform development, and default settings have a profound impact on individuals' privacy, access to information and data rights such as the freedom from manipulation and coercion.

These decisions will define the control individuals and communities have over their rights, which will subsequently affect their level of trust for online services. This principle seeks to reflect the reality of companies' importance to the realization of privacy and data rights. The aim of establishing this principle and clauses is to make them commit and thus accountable for documenting adverse rights impacts that arise as a result of their operations, providing strong default privacy settings and alternatives, and providing clear ways for an individual to exercise their data rights.

HUMAN RIGHTS FRAMEWORK

Privacy and other data rights have their basis in pre-existing human rights frameworks. The respect and protection of these international frameworks, interpreted to reflect the digital age, provide the strongest basis from which to base the contractual principles. Reflecting that other areas of the contract provide a basis from which to understand wider rights of access to information and openness, the core rights at play in privacy and other data rights are:

Article 12 of the Universal Declaration of Human Rights (UDHR): 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

"In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files."

– **Human Rights Committee**, General Comment 16, adopted on 8 April 1988

Article 17 of the International Covenant on Civil and Political Rights (ICCPR): 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.'

"A central part of human rights due diligence as defined by the Guiding Principles [on Business and Human Rights] is meaningful consultation with affected stakeholders. In the context of information and communications technology, this also includes ensuring that users have meaningful transparency about how their data are being gathered, stored, used

and potentially shared with others, so that they are able to raise concerns and make informed decisions.”

- **Office of the High Commissioner of Human Rights**, 30 June 2014 ([A/HRC-27-37](#))

Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

- (1) Everyone shall have the right to hold opinions without interference.
- (2) Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

“Among the most important steps that private actors should take is the development and implementation of transparent human rights assessment procedures... Such assessments should critically review the wide range of private sector activities in which they are engaged, such as the formulation and enforcement of terms of service and community standards on users’ freedom of expression...; the impact of products, services and other commercial initiatives on users’ freedom of expression as they are being developed, including design and engineering choices, and plans for differential pricing of or access to Internet content and services...”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 11 May 2016 ([A/HRC/32/38](#))

OTHER EXISTING FRAMEWORKS

Beyond the core Human Rights International Legislation mentioned above (UDHR and ICCPR), we also consider the following existing frameworks:

Guiding Principles on Business and Human Rights:

The Principles — endorsed by the United Nations Human Rights Council — provide a global standard for preventing and addressing the risk of adverse impacts on human rights linked to business activity. Relevant principles include the responsibility to respect human rights which requires due diligence on the part of the company. This involves becoming aware of, preventing and addressing adverse human rights impacts.

EU General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the Council¹, the European Union’s (“EU”) new General Data Protection Regulation (“GDPR”), regulates the processing by an individual, a company or an organization of personal data relating to individuals in the EU.

Global Network Initiative Principles on Freedom of Expression and Privacy:

The principles provide guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of human rights globally, they have also been called as a framework by the Special Rapporteur on Freedom of Opinion and Expression as a minimum set of principles for companies to adhere to. Developed by companies, investors, civil society organizations, and academics, the principles seek to establish that rights to freedom of expression and privacy should be respected by Governments and that companies should respect and work to protect these fundamental rights.

Organization for Economic Cooperation and Development Guidelines on Multinational Enterprises:

The OECD Guidelines on Multinational Enterprises are recommendations addressed by governments to multinational enterprises operating in or from adhering countries. They provide non-binding principles and standards for responsible business conduct in a global context consistent with applicable laws and internationally recognized standards. The principles include a chapter on Consumer Interests where enterprises should respect consumer privacy and take reasonable measures to ensure the security of personal data that is collected, stored, processed, or disseminated, and provide consumers with access to fair, easy to use, timely and effective non-judicial dispute resolution and redress mechanisms.

WORKING GROUP

D: Positive Technology

List of members: <http://wfcontract.wpengine.com/positive-tech/>

Chairs: Derek Slater & Juan Ortiz Freuler

External Expert: Joana Varon

PRINCIPLE 6

[Companies will]: Develop technologies that support the best in humanity and challenge the worst

So the web really is a public good that puts people first

CONTEXT

As the Web has become more important to the economy and society, it is ever more important to consider social impacts in the design and the deployment of new web based technologies. Therefore, development and implementation of web technologies should take into account more than serving an individual user's interests but consider the collective promotion and protection of human rights, as well as addressing sustainable development goals.

Responsible design of web technologies does not follow a single, simple formula. However, it can be shaped by developing a shared set of guiding principles, and substantive constraints. Steps should therefore be taken to ensure that web based technologies are developed and deployed in a way that is inclusive, accountable, transparent and seek social justice.

This Principle is focused on the frameworks, methods and metrics that might best guide developers, civil society and governments in working together to foresee and solve the problems they might create, as well as harnessing the affordances of the web towards ensuring positive outcomes.

HUMAN RIGHTS FRAMEWORK

Principle 6

The protection and promotion of Human Rights and the web's architecture and technical design choices are interconnected. Acknowledging that other sections of the contract specifically address the rights to privacy and accessibility, we understand the norms proposed under Principle 6 are rooted in human rights, such as:

Preamble to the International Covenant on Economic, Social and Cultural Rights (ICESCR):

'Recognizing that, in accordance with the Universal Declaration of Human Rights, the ideal of free human beings enjoying freedom from fear and want can only be achieved if conditions are created whereby everyone may enjoy his economic, social and cultural rights, as well as his civil and political rights.'

"The Guiding Principles [on business and human rights] establish a framework according to which companies should, at a minimum:

- (a) *Avoid causing or contributing to adverse human rights impacts and seek to prevent or mitigate such impacts directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts (principle 13);*

- (b) *Make high-level policy commitments to respect the human rights of their users (principle 16);*
- (c) *Conduct due diligence that identifies, addresses and accounts for actual and potential human rights impacts of their activities, including through regular risk and impact assessments, meaningful consultation with potentially affected groups and other stakeholders, and appropriate follow-up action that mitigates or prevents these impacts (principles 17–19);*
- (d) *Engage in prevention and mitigation strategies that respect principles of internationally recognized human rights to the greatest extent possible when faced with conflicting local law requirements (principle 23);*
- (e) *Conduct ongoing review of their efforts to respect rights, including through regular consultation with stakeholders, and frequent, accessible and effective communication with affected groups and the public (principles 20–21);*
- (f) *Provide appropriate remediation, including through operational-level grievance mechanisms that users may access without aggravating their “sense of disempowerment”(principles 22, 29 and 31)."*

– **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**, 6 April 2018 ([A/HRC/38/35](#))

“The integration of human rights policies throughout a company may be the biggest challenge in fulfilling the corporate responsibility to respect. As is true for States, human rights considerations are often isolated within a company. That can lead to inconsistent or contradictory actions: product developers may not consider human rights implications; sales or procurement teams may not know the risks of entering into relationships with certain parties; and company lobbying may contradict commitments to human rights. Leadership from the top is essential to embed respect for human rights throughout a company, as is training to ensure consistency, as well as capacity to respond appropriately when unforeseen situations arise.”

- **John Ruggie** - Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 7 April 2018 ([A/HRC/8/5](#))

“Public consultations and engagement should occur prior to the finalization or roll-out of a product or service, in order to ensure that they are meaningful, and should encompass engagement with civil society, human rights defenders and representatives of marginalized or underrepresented end users. The results of human rights impact assessments and public consultations should themselves be made public.”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 29 August 2018 ([A/73/348](#))

Article 19 of the Universal Declaration of Human Rights (UDHR): ‘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.’

“Ensuring an internet free from gender-based violence enhances freedom of expression... as it allows women to fully participate in all areas of life and is integral to women’s empowerment... Online gender-based abuse and violence are undeniably a scourge, and governments and companies should be taking action against it.”

- **Joint Communiqué** by Dubravka Šimonović - Special Rapporteur on violence against women and David Kaye - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

“Terms of service should move away from a discretionary approach rooted in generic and self-serving “community” needs. Companies should instead adopt high-level policy commitments to maintain platforms for users to develop opinions, express themselves freely and access information of all kinds in a manner consistent with human rights law. These commitments should govern their approach to content moderation and to complex problems such as computational propaganda.”

- **David Kaye** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 ([A/HRC/38/35](#))

Article 7 of the Universal Declaration of Human Rights (UDHR): ‘... All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.’

“Business enterprises in the ICT sector should embed gender equality and diversity as core values across organizational and employment policies...”

States and business enterprises should act to prevent and combat online violence against women. They should collect comprehensive data on the extent and nature of online violence against women and conduct further research to understand and address its underlying causes and how best to combat it. Civil society should monitor this data collection to ensure it is done in an effective and gender-sensitive manner...

When involved in content moderation, business enterprises, including Internet intermediaries, should put in place clear, transparent and proportionate procedures, respecting human rights, in particular women’s rights, and the rights to privacy and to freedom of opinion and expression. Relevant staff, both female and male, should be trained accordingly. Business enterprises should ensure that information about their terms of service and how these are enforced is adequate, understandable and easily available to all users.”

- **Report of the United Nations High Commissioner for Human Rights**, 5 May 2017 ([A/HRC/35/9](#))

Article 27 of the Universal Declaration of Human Rights (UDHR): ‘Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.’

“With the Internet emerging as a critical platform for scientific and cultural flows and exchanges, freedom of access to the Internet and maintaining its open architecture are important for upholding the right to participate in cultural life and to enjoy the benefits of scientific progress and its applications.”

- **Frank La Rue** - Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 May 2011 ([A/HRC/17/27](#))

OTHER EXISTING FRAMEWORKS

Beyond the core International Human Rights law and The [2030 Agenda for Sustainable Development](#), the following existing frameworks are particularly informative:

RFCs from the Working group at the IETF about Human Rights Protocol Consideration: The Human Rights Protocol Considerations Research Group is chartered to research whether standards and protocols can enable, strengthen or threaten human rights, specifically, but not limited to the right to freedom of expression and the right to freedom of assembly. As an exercise to translate technical terms into human rights, it might be an important initiative to keep track as it has the goal to provide guidelines to inform future protocol development and decision making where protocols impact the effective exercise of the right to freedom of expression or association.

OECD Guidelines for Multinational Enterprises: Recommendations addressed by governments to multinational enterprises operating in or from adhering countries. They provide non-binding principles and standards for responsible business conduct in a global context consistent with applicable laws and internationally recognized standards.

WORKING GROUP

E: Public Action

List of members: <https://contractfortheweb.org/public-action/>

Chairs: Sharon Johnson & Adrian Lovett

Rapporteur: Juan Ortiz Freuler

PRINCIPLE 7**[Citizens will]: Be creators and collaborators on the web**

So the web has rich and relevant content for everyone

PRINCIPLE 8**[Citizens will]: Build strong communities that respect civil discourse and human dignity**

So that everyone feels safe and welcome online

PRINCIPLE 9**[Citizens will]: Fight for the web**

So the web remains open and a global public resource for people everywhere, now and in the future

CONTEXT

The web was built as an open platform; one that would evolve based on the aggregate set of decisions made by the decentralized masses of people who would publish content on it, and link existing pieces of content together. By people who would discuss and create new standards for its architecture. This decentralized design is increasingly at risk. For the web to remain healthy and aligned with the public interest, we need to bolster public engagement. We need the citizens to remain the key driving force behind the web. As we reach a point in which 50% of the world is connected, this becomes more important than ever. We need the next 50% to join a space that empowers them and enables them to thrive.

These principles are focused on developing an understanding of our digital citizenship, and the ways in which we can and should step up to the challenge of ensuring the web remains open for everyone. It includes components that aim to foster civic behavior online, as well as mechanisms for people to develop a better understanding of how the web works and how they can fight for it.

HUMAN RIGHTS FRAMEWORK

Article 1 of the Universal Declaration of Human Rights (UDHR): 'All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.'

Article 29.1 of the Universal Declaration of Human Rights (UDHR): 'Everyone has duties to the community in which alone the free and full development of his personality is possible.'

Preamble to the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR): 'Realizing that the individual, having duties to other individuals and to the community to which he belongs, is under a responsibility to strive for the promotion and observance of the rights recognized in the present Covenant.'

OTHER EXISTING FRAMEWORKS

https://www.educationworld.com/a_tech/responsible-student-technology-use.shtml

<https://www.wikihow.com/Be-a-Responsible-Digital-Citizen>

<http://www.digitalcitizenship.net/nine-elements.html>

Glossary:

This section provides a set of references that may help those seeking to understand the technical terminology used in the Contract.

At the end of each definition, there is a reference to the key Principles to which each definition relates:

Governments: **PRINCIPLES 1-3** Companies: **PRINCIPLES 4-6** Citizens: **PRINCIPLES 7-9**

Affordability of internet access: the extent to which internet use is limited by the cost of access relative to income levels (Source: [A4AI 2018 Affordability Report](#)).

PRINCIPLE 1

Barriers for people with disabilities: limitations faced by people with varied hearing, movement, sight, and cognitive abilities in the ways they can navigate the internet, contribute to and enjoy the tools made available through it ([UNESCO](#)). - Also see “Web Accessibility.” **PRINCIPLE 4**

Civil discourse: engagement in conversation with the purpose of enhancing understanding. It requires respect of the other participants; avoids hostility, direct antagonism, or excessive persuasion; it requires modesty and an appreciation for the other participant’s experience (Source: K.J. Gergen -Read More: [Wikipedia](#)).

PRINCIPLE 7 **PRINCIPLE 8** **PRINCIPLE 9**

Community networks: telecommunications infrastructure deployed and operated by a local group to meet their own communication needs. They are the result of people working together, combining their resources, organizing their efforts, and connecting themselves to close connectivity and cultural gaps (Source: [ISOC](#), based on [DCCC IRTF](#)). **PRINCIPLE 1**

PRINCIPLE 4

Competent and independent judicial authority: an impartial and independent authority, conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights involved, and adequately resourced to exercise those functions (Source: [Necessary and Proportionate](#), pg. 6).

PRINCIPLE 3

Data: an interpretable representation of information in a formalized manner suitable for communication, interpretation, or processing (Source: [ISO](#)). **PRINCIPLE 3**

PRINCIPLE 5

Data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed (Source: [GDPR](#), Article 4(12)). **PRINCIPLE 3**

Digital literacy: the skills and capabilities needed to participate fully, effectively and equally in our digital world (Source: [Web Foundation](#)). **PRINCIPLE 1**

Dig once regulations: “refers to policies that allow for and/or encourage deployment of conduit and fiber in transportation rights of way during other infrastructure improvement projects. This can include, for example, installing pipes under roadbeds that can house numerous internet cables. Rather than digging up the road each time a new company wants to install high-speed internet cables, the Dig Once infrastructure would permit companies access to their cables, allowing for upgrades and additions as needed” (Source: [IEEE](#)).

PRINCIPLE 1

Diversity: diversity means understanding that each individual is unique, and recognizing our individual differences, which include but are not limited to age, ethnicity, class, gender, physical abilities/qualities, race, sexual orientation, national origin, religious status, gender expression, educational background, geographical location, income, marital status, parental status, work experiences, among others (Source: [UN: Delivering successful change on diversity and inclusion in the UN](#)). **PRINCIPLE 6**

Gender inclusive: a process that refers to how well different gender identities are included as equally valued players in initiatives. Gender-inclusive projects, programmes, political processes and government services are those which have protocols in place to ensure all genders are included and have their voices heard and opinions equally valued (Source: Adapted from [UNDP](#)). Inclusion policies have become key to close the measurable gap between women and men in their access to, use of and ability to influence, contribute to and benefit from ICTs ([A/HRC/35/9](#)). **PRINCIPLE 1**

PRINCIPLE 4 **PRINCIPLE 6**

Gender responsive: refers to outcomes that reflect an understanding of gender roles and inequalities and which make an effort to encourage equal participation and equal and fair distribution of benefits (Source: [UNDP](#)). **PRINCIPLE 1** **PRINCIPLE 4**

Human Rights: “Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status. Human rights include the right to life and liberty, freedom from slavery and torture, freedom of opinion and expression, the right to work and education, and many more. Everyone is entitled to these rights, without discrimination (Source: [United Nations](#)). **Relevant to all Principles.**

Individual profiling: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements (Source: [GDPR](#), Art. 4(4)).

PRINCIPLE 3 **PRINCIPLE 5**

Inferred data: personal data that is usually derived or assigned to an individual from interpretations of other data shared by the individual and/or collected through observation of the individual’s use of an online service or device, including connected objects (Source: [EU Guidelines on the right to data portability](#), pg. 10).

PRINCIPLE 3 **PRINCIPLE 5**

Infrastructure sharing: sharing telecommunications infrastructure (such as towers, high sites, ducts, fibre cables, antennas or transmission components) by competing operators (Source: [IFC](#)). **PRINCIPLE 1**

Infrastructure sharing (active): the sharing of active elements in the radio access network such as antennas and radio network controllers (RNC). National roaming is a form of active sharing (Source: [BEREC](#)). **PRINCIPLE 1**

PRINCIPLE 4

Infrastructure sharing (passive): is the sharing of the passive elements of network infrastructure such as masts, sites, cabinet, power, and air conditioning (Source: [BEREC](#)). **PRINCIPLE 1** **PRINCIPLE 4**

Interoperability: the ability of different types of computers, networks, operating systems, and applications to work together effectively, without prior communication, in order to exchange information in a useful and meaningful manner (Source: [DC](#)). **PRINCIPLE 2**

PRINCIPLE 6

Legality: restrictions [to art. 19.3 of the ICCPR, regarding the right to freedom of expression] must be “provided by law”. In particular, they must be adopted by regular legal processes and limit government discretion in a manner that distinguishes between lawful and unlawful expression with “sufficient precision”. Secretly adopted restrictions fail this fundamental requirement. The assurance of legality should generally involve the oversight of independent judicial authorities (Source: [A/HRC/38/35](#)). **PRINCIPLE 2**

Legitimate public interest: a set of values corresponding to an important legal interest that is necessary in a society, often including, public safety, protection of public order, health and morals, the protection of rights and freedoms of others (Source: [ECHR](#), Article 8(2)). **PRINCIPLE 3**

Meaningful connectivity: a new global standard that measures not only if someone has accessed the internet, but the quality of connection they have (Source: [A4AI](#)). **PRINCIPLE 1**

Necessity and Proportionality: any restriction [to art. 19.3 of the ICCPR, regarding the right to freedom of expression] should create the least burden on the exercise of the right and actually protects, or is likely to protect the legitimate State interest at issue. States may not merely assert necessity but must demonstrate it, in the adoption of restrictive legislation and the restriction of specific expression (Source: [A/HRC/38/35](#)).

PRINCIPLE 2

Observed data: personal data that is provided through an individual's use of an online service or device, including connected objects. Examples include search history, traffic data, location data or heartbeat (Source: [EU: Guidelines on the right to data portability](#)).

PRINCIPLE 3 PRINCIPLE 5

Online privacy: a sphere of autonomy in which individuals and communities can explore the Web free from private actors' and Government's coercion, control, interference or surveillance (Source: [Contextualization of Lord Lester and D. Pannick \(eds.\), Human Rights Law and Practice, 2004, para. 4.82](#) adding the reference to the Web and freedom from interference by private actors).

PRINCIPLE 3 PRINCIPLE 5

Open access rules: all suppliers are able to obtain access to the network facilities on fair and equivalent terms ([ITU](#)).

PRINCIPLE 1

Open data: "Open data is digital data that is made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere." (Source: [Open Data Charter](#)).

PRINCIPLE 6

Open knowledge: "Knowledge anyone is free to access, use, modify, and share it — subject, at most, to measures that preserve provenance and openness." (Source: [Open Definition](#)).

PRINCIPLE 6 PRINCIPLE 7

PRINCIPLE 8 PRINCIPLE 9

Open license: a document that specifies that a work (be it sound, text, image or multimedia) is free for anyone to print out and share, publish on another channel or in print, make alterations or additions, incorporate, in part or in whole, into another piece of work, use as the basis for a work in another medium, and other freedoms (Source: [Open Definition](#) - Read More: [Wikipedia](#)).

PRINCIPLE 7 PRINCIPLE 8 PRINCIPLE 9

Open source software: software distributed under terms that include the right to: free redistribution of the source code, access and reuse of the source code, including the creation of derived works to be distributed under the same license (with a series of exceptions only if the license allows the distribution of "patch file). OSS, by definition, must not discriminate against persons or groups, or against fields of endeavor. The rights attached to the program must apply to all to whom the program is redistributed, and must not be specific to a product or restrict other software. Licenses must be technology-neutral (Source: Adapted from [OSI](#); Read More: [Wikipedia](#)).

PRINCIPLE 7 PRINCIPLE 8 PRINCIPLE 9

Open source technology: see "Open source software"

Open standard: a formal document that establishes uniform technical criteria, and is developed through an open, consensus driven, participatory process, focused on supporting interoperability (Source: [W3C/IEEE](#); with edits based on [Ken Krechmer](#) - Read More: [Wikipedia](#)).

PRINCIPLE 6 PRINCIPLE 7 PRINCIPLE 8 PRINCIPLE 9

Open Web: This includes two components, a technical and a legal one. Technical: development of web technologies in accordance with the open standards developed by the World Wide Web Consortium (W3C), which ensures interoperability across web browsers. Legal: Absence of laws or regulations that restrict people from accessing web content or other web-based technologies over the internet.

PRINCIPLE 7 PRINCIPLE 8

PRINCIPLE 9

Personal data: any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Source: [GDPR, Article 4\(1\)](#)).

PRINCIPLE 3 PRINCIPLE 5

Privacy / data protection by design: a holistic approach incorporating technology and policy development that places privacy as a central component at the beginning of every service design process (Source: [EU Resolution on Privacy by Design and GDPR](#)).

PRINCIPLE 5

Public registers: a published list made available online and updated regularly. In this particular context the registers must contain general information on data sharing and/or purchase agreements across the public sector and industry, explaining the types of data that are being shared or purchased, the recipient(s), and purpose(s). Additionally these registers must provide a reference source with general information on data breaches from public and private sources, including the organizations and data categories affected (Source: Inspired by Article 30, [Anti-Money Laundering Directive](#) with significant expansion and contextualization from the Working Group, in particular bringing the types of agreements that are expected to be provided within the registers and the information provided alongside them).

PRINCIPLE 3 PRINCIPLE 5

Quality of service: in the case of Internet access, quality of service measures not only include speeds, but also delay, jitter, availability, and packet loss (Source: [A4AI QoS](#), GSMA). **PRINCIPLE 4**

Radio spectrum : the radio frequency spectrum of hertzian waves allocated based on guidance from the ITU, and used as a transmission medium for cellular radio, satellite communication, over-the-air broadcasting and other communication services (Source: [ITU](#)). **PRINCIPLE 1**

Standard technology: see “Open Standard”

Sustainable Development Goals: the 2030 Agenda for Sustainable Development, adopted by the UN in 2015 sets 17 goals: no poverty, zero hunger, good health and well-being, quality education, gender equality, clean water and sanitation, affordable and clean energy, decent work and economic growth, industry innovation and infrastructure, reduced inequalities, sustainable cities and communities, responsible production and consumption, climate action, life below water, life on land, peace, justice and strong institutions and partnerships for the goals (Source: [UN SDGs](#)). **PRINCIPLE 6**

Universal service: ensuring every individual within a country has basic internet access service available at an affordable price (Source: adapted from [WTO](#)). **PRINCIPLE 1**

Universal Service and Access Funds (USAFs): are communal public funds dedicated to expanding internet connectivity and access opportunities for those least likely to be connected through market forces alone (Source: [A4AI](#)). **PRINCIPLE 1**

User interface: all components of an interactive system (software or hardware) that provide information and controls for the user to accomplish specific tasks with the interactive system (Source: [ISO](#)). **PRINCIPLE 4**
PRINCIPLE 5 **PRINCIPLE 6**

Web accessibility: web technologies that work for all people, whatever their hardware, software, language, location, or ability. When the Web meets this goal, it is accessible to people with a diverse range of hearing, movement, sight, and cognitive ability (Source: [W3C](#)). **PRINCIPLE 1** **PRINCIPLE 4** **PRINCIPLE 7** **PRINCIPLE 8**
PRINCIPLE 9

Web technologies: a set of computing technologies that together provide a realization of the “Architecture of the World Wide Web” (Source: [W3C](#)). **PRINCIPLE 6**

Acknowledgments:

The Contract for the Web, like the web itself, is a collective endeavor. As such, it could not have been achieved without the insights, comments, suggestions and critiques from a number of actors. In particular we want to thank:

The Contract for the Web Core Group that acted as a steering committee during the process:

Chair: José M. Alonso (Web Foundation)

Participants: Adrian Lovett (Web Foundation), Antoine Jourdan (Government of France), Besart Copa (Pango), Derek Slater (Google), Emily Sharpe (Web Foundation), Fadi Quran (Avaaz), Jamal Edwards (Microsoft), Jan Gerlach (Wikimedia Foundation), Juan Ortiz Freuler (Web Foundation), Kaja Ciglic (Microsoft), Kirsten Rulf (Government of Germany), Lillian Nalwoga (CIPESA), Maximilian Senges (Google), Nathan Miller (Avaaz), Nnenna Nwakanma (Web Foundation), Sharon Johnson (The New Now), Stephen LaPorte (Wikimedia Foundation), and Wairagala Wakabi (CIPESA).

The 600+ people that submitted comments and suggestions during the [public participation phase](#).

The thousands of people who backed the Contract for the Web Principles and who shared their views of what should be included in the Contract for the Web.

All the members of the Communications, Research and Policy teams at Web Foundation, for their support throughout, and particularly to project officer Daphnee Iglecias.

**_ For
The
Web**