Draft July - A Contract for the Web

Draft 1: July 2019

This is a working draft document reflecting contributions from a range of participants. Given this document is still in the process of negotiation, at this stage participants have not been asked to formally support or oppose the document in its current form. We look forward to working with others to finalise the document.

To provide feedback on this draft text, complete the public survey by September 8, 2019.

The Contract Draft is available to read in Español (Spanish) **and** Português (Portuguese)**.**

Table of Contents

The web was designed to bring people together and make knowledge freely available. Everyone has a role to play to ensure the web serves humanity. By committing to this Contract, governments, companies and citizens around the world can help protect the open web as a public good and a basic right for everyone.

Governments will

Principle 1 – 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 ambitious policy goals:

1. 1GB of mobile data costs no more than 2% of average monthly income by 2025.
2. At least 70% of youth over 10 years old and adults have ICT skills by 2025.
3. Access to broadband internet (speeds that make it possible to access or deliver new content, applications and services) is available for at least 90% of citizens by 2030, and the gap towards that target is halved by 2025.

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

1. 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.
2. Cost effective access to critical infrastructure.
3. Institutions with capacity to ensure compliance with laws and regulations designed to foster Internet adoption.
4. Open access rules on wholesale infrastructure in non-competitive areas, and access to license-exempt spectrum.
5. Tax and investment policies that stimulate rapid investment in, and adoption, of connectivity solutions, such as reducing taxes and import duties on telecommunications/ICT equipment and services.

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

1. Implementing national broadband policies with specific actions to target excluded populations.
2. Funded broadband strategies are adopted and Internet access is supported in public policy, including universal access and services definition, with effective technology neutral financing mechanisms for network development in underserved areas.
3. Support the local production of content and applications, and the development of the necessary infrastructure and enabling environment for accelerating the growth of digital businesses. This ranges from support for establishing local innovation hubs and data hosting centres, to minimizing taxes on ICT equipment and services and equipping citizens with e-skills through training and education to improve digital literacy.
4. Designing inclusive policies to increase internet access and digital literacy of women, other marginalized gender identities and other under-represented or disadvantaged populations.

Principle 2 – 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 aimed at minimizing government-triggered internet disruptions:

1. 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 national borders.
2. Engaging in transparent and documented coordination with private sector actors to ensure that any attempts to restrict access to 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.

3. Ensuring all government content take-down requests are based 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.

2. By creating capacity to ensure demands to remove illegal content are done in ways that are consistent with Human Rights Law:

1. 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.
2. Funding research and engaging in multi stakeholder forums aimed at aligning potential regulation of content take-down and moderation dispute resolution mechanisms with human rights standards.
3. Researching and documenting the cost of service interruptions to the national economy, business and users.

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

1. 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.
2. 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.
3. Funding research to determine the degree and character of competition and/or consolidation online, and its impact.

Principle 3 – 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:

1. the principle of meaningful, freely given, informed, specific and unambiguous consent for the processing of personal data, without excluding any other possible legal basis for data processing when reasonable.
2. 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.

3. 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.
4. 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.
5. 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.
6. the right to redress through an independent complaints mechanism 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:

1. made under clearly defined laws subject to a competent judicial authority that includes avenues for redress.
2. restricted to those cases where there is a legitimate public interest defined in law.
3. 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:

1. minimising their own data collection to what is adequate, relevant, and necessary to achieve a clearly specified public interest.
2. 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.
3. 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.
4. 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 taking enforcement actions when appropriate.

Companies will

Principle 4 – 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:

1. Designing gender responsive and economically inclusive data plans.
2. Supporting the development of Community Networks, particularly in unserved and underserved areas.
3. 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 in order to enable every person, when accessing the internet, to use email addresses and domain names that are in their native languages and writing systems.

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

1. Documenting and publishing their investments and best efforts approach towards ensuring the speed, reliability and performance of their networks.
2. 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.
3. 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:

1. Crafting corporate policies that minimise access barriers created by differences in language, location, age and ability.
2. Ensuring that applications and services are designed with potentially excluded groups.
3. Designing gender inclusive strategies to increase internet access and digital literacy by women, marginalized gender identities and other under-represented or disadvantaged populations.

Principle 5 – 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:

1. providing clear explanations of processes affecting users' data and privacy and their purpose.
2. providing control panels where users can manage their data and privacy options in a quick and easily accessible place for each user account.
3. 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:

1. minimising data collection to what is adequate, relevant, and necessary for the provision of the service requested by the user.
2. 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.
3. 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.
4. 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:

1. providing dedicated and readily available mechanisms for individuals to report adverse privacy and data protection impacts directly linked to company's operations, products or services —which the company should address and mitigate as required by law.
2. promoting innovative business models that strengthen data rights, respect privacy, and minimise data collection practices.
3. providing clear and understandable privacy policies and consent forms, where the types of personal data processed are listed, and the data collection purposes are explained.
4. clearly and directly communicating any updates and changes regarding privacy policies.

Principle 6 – 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:

1. Respecting and supporting human rights, as outlined by the UN Guiding Principles on Business and Human Rights.
2. Establishing policies and partnerships designed to respect and promote the achievement of the Sustainable Development Goals, particularly those pertaining to education, gender equality, marginalized communities, climate, and socio-environmental justice.
3. Socially beneficial and how they assess and address foreseeable risks created by their technologies, including with respect to online content, behaviour, and personal well-being.

2. By engaging with communities in an inclusive way:

1. 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.
2. Ensuring a diverse workforce: releasing periodic reports including metrics that show progress towards a more representative workforce.
3. 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 and supporting the digital commons:

1. Upholding and further developing open web standards.
2. The promotion of interoperability, open-source technologies, open access, open knowledge, and open data practices and values.
3. Ensuring the terms of service, interfaces and channels of redress are accessible and available in local languages and formats that allow and encourage a diverse set of users to actively participate and contribute to the commons.

Citizens will

Principle 7 – Be creators and collaborators on the web

So the web has rich and relevant content for everyone.

1. By being active participants in shaping the web, including content and systems made available through it, such as by:

1. Promoting and using open licenses to share information of public interest.
2. Sharing best practices and guidelines to help create and develop a web focused on prioritising the needs of citizens.
3. Advocating for standard technology that is open and accessible to all persons, regardless of their abilities.
4. Producing content in local or minority languages.

Principle 8 – Build strong communities that respect civil discourse and human dignity

So that everyone feels safe and welcome online.

1. By working towards a more inclusive web:

1. Adopting best practices on civil discourse online and educating the next generation on these matters.

2. Committing to amplify the messages of systematically excluded groups, and standing up for them when they are being targeted or abused.
3. Taking steps to protect their privacy and security, and that of others, by choosing products and services thoughtfully, and expressing privacy preferences accordingly.
4. Refraining from participating in the non-consensual dissemination of intimate information that breach privacy and trust.

Principle 9 – Fight for the web

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

1. By being active citizens of the web, including:

1. Creating awareness amongst peers regarding threats to the open web
2. Opposing the web's weaponization by nation states or any other entity.
3. Supporting organizations, processes and people who promote the open web.
4. Supporting startups and established companies that care about the web's future.
5. Engaging political representatives and companies to ensure support and compliance with this Contract and support for the open web.

To provide feedback *on this draft text, complete the public survey by September 8, 2019.*