Access Now response to ITU Consultation: **Building an enabling environment for access to the Internet**

http://www.itu.int/en/council/cwg-internet/Pages/consultation-feb2016.aspx

1. *What are the elements of an enabling environment to promote Internet **connectivity**?*

Universal access to the internet is a paramount goal of all stakeholders in the digital age. Without the internet, more than four billion people lack access to the 21st century's essential global forum for expression, communication, information, innovation, and wealth creation. Accordingly, the U.N.'s ambitious "Global Goals for Sustainable Development" rightly emphasize that access to technology underpins every other "Global Goal" toward the eradication of extreme poverty.

However, not all connectivity is the same, or yields the same benefits to societies in terms of economic, social, or cultural development. Only stable, secure, and open access to broadband internet will ensure the implementation and achievement of the United Nations (UN) Sustainable Development Goals (SDGs). As noted in a joint civil society statement to finance ministers at the 2016 Spring Meetings of the International Monetary Fund and the World Bank Group,[1] information and communications technologies (ICTs) are vectors of economic and social transformation and economic growth. Based on the data of the Inter-American Development Bank, with every 10 percent increase in high speed internet connections, economic growth increases by 3.2 percent, and at the global level, according to the Word Bank, the average increase is 1.3 percent. Yet the majority of people lack access to the internet, and digital divides along gender, socioeconomic, and geographic lines persist.

New research reveals another factor closely correlated with connectivity: political power. According to a study published recently in Science,[2] Nils Weidmann, a professor of political science at the University of Konstanz in Germany, and other researchers found that "politically excluded groups suffer from significantly lower Internet penetration rates compared with those in power, an effect that cannot be explained by economic or geographic factors." This research shows the importance of policy environments that foster inclusion and non-discrimination, and seek to overcome political obstacles that isolate and marginalize societal groups.

Acknowledging the difficulty of extending connectivity to all, Access Now and more than 20 other organizations (http://bestbits.net/finance-ministers-global-connect) have identified a number of measures for development banks and national and regional authorities to take to expand internet access. Recommendations:

- Integrate internet connectivity and access to digital technologies ("ICT infrastructure") as key components of national development, borrowing, and investment strategies;

[1] http://bestbits.net/finance-ministers-global-connect
[2] http://science.sciencemag.org/content/353/6304/1151

- Foster the growth of internet connectivity by urging national development agencies to prioritize digital access as an essential element of national infrastructure plans and investing sufficient funds for implementation;
- Invest in increasing technical expertise in digital connectivity at national and local levels;
- Invest in internet connectivity based on a core understanding that the internet is a global resource and that it should be managed in the public interest as a democratic, secure, free, open, inclusive and pluralistic communication platform;
- Support public access facilities, such as libraries, which facilitate significant gains in connectivity and sustainable development;
- Support and invest in unlicensed and open spectrum, to expand connectivity within a community, to additional homes and institutions;
- Create enabling environments by adopting policies and strategies that focus not only on spurring connectivity, but also entrepreneurship, cross-border information flows, and open and competitive marketplaces;
- Invest in and adopt more effective policies that ensure: equitable and efficient access to radio spectrum; infrastructure sharing and lower barriers to entry for access providers with new technologies; better and targeted subsidies, direct investment in infrastructure roll out; and more transparent and accountable public-private partnerships.

*2. What are the elements of an enabling environment to promote an **affordable** Internet?*

The Alliance for Affordable Internet (A4AI) has studied the issue at length, and identified a number of factors reducing affordability, in a diverse range of countries. The A4AI studies find that affordability is a key problem slowing progress toward achieving the Sustainable Development Goals (SDGs), and warns of the potential risks to miss the 2020 target for universal and affordable access in the world's least developed countries by 22 years. Often, access to the internet costs disproportionately more, as a percentage of income, in countries where the quality of internet access remains poor. This rather backwards reality deters the wider adoption of broadband internet services, and slows progress for both economic development and the realization of human rights. The A4AI study also highlights the impact of the gender pay gap on affordability as the cost to connect is higher for women living in poverty and at the bottom of the income pyramid. The gender wage gap diminishes the ability of women — and female-headed households in particular — to afford Internet access.

The inequality and gaps that characterize current penetration and connection rates also reveal an untapped development opportunity. Simply put, internet connectivity and public access must become an integral part of national development policies moving forward in order to ensure the benefits of the digital economy spread to all. Connectivity consistent with human rights principles should be an essential element in every grant, loan, technology transfer, or policy-training program that international institutions facilitate.

Recommendations: We support the findings of the 2015 report[3] by A4AI, including to unite around an ambitious affordability benchmark, such as "1 for 2", or "1GB of data priced at 2% or less of average monthly income"; reducing the cost of devices, through tax and patent relief, as well as pressure on equipment providers; increased investment in and subsidies for public access points; specific targets to close the gender divide, including through funding for capacity building programs; and transparent, inclusive policy development process that align the goals of all stakeholders and institutions.

Additionally, promoting the use and development of open source software and open licensing also can reduce costs and barriers to entry. Reliance on proprietary systems, and use of restrictive licensing, reduces opportunities for innovation, increases "lock-in" to long term contracts, and can raise the cost of infrastructure maintenance in the long-term.

*3. What are the elements of an enabling environment to promote the **quality** of access to the Internet?*

Increasing connectivity cannot form the sum of global policy on ICTs and development. Respect for privacy and the freedom of expression must go hand in glove with the drive to connection. Global leaders should embrace the challenge of building a framework for human rights in the digital age that allows the internet's current billions and next 4 billion users to connect seamlessly, securely, affordably, and openly. Respect for human rights must be baked into the connectivity agenda from the start.

Measures to ensure better quality connections include capacity-building programs to foster digital literacy, and enable and promote the development of locally relevant content, applications, and services, as they are essential to widespread adoption of the internet and increase its social and economic value to people, families, and communities.

Protecting the open nature of the internet is compatible with – if not an absolute prerequisite for – the availability and the development of the Internet of Things and the ever-increasing number of innovative products and services, such as connected cars and e-health. In fact, the principles on which net neutrality is based, including innovation without a need to obtain permission, end-to-end connectivity, transparency, and non-discrimination, are essential for these innovative products and services. Since these products often rely on significant and constant bandwidth, regulation protecting access to the unfettered internet will be needed.

With global demand for faster and better access to the internet on the rise, internet access providers will continue to have a strong incentive to develop and invest in enhanced network capacity. This so-called "virtuous circle" illustrates the long-term economic benefit for telecommunications companies to invest in infrastructure. It is crucial for governments to ensure users' access to the internet but also offer the highest quality of connectivity possible, not only in terms of speed but also in security, privacy and openness.

[3] http://a4ai.org/affordability-report/report/2015/#executive_summary

The development of high-quality network must benefit the internet as a whole, and only few players in the market. In that sense, zero rating — the practice of offering internet users free access to some, but not all, of the internet, resulting in unequal access — is currently one of the biggest threat to connectivity and the open internet. Zero rating fails to respect Net Neutrality, the notion that all traffic on the internet should be treated equally. Net Neutrality is central to maintaining the internet's potential for economic and social development, and to the exercise of human rights such as the right to free expression and freedom of information. Zero rating is a form of "network discrimination" which deliberately sets up a system where "the internet" provided is different for different people. Zero rating programs manifest in different forms but all have in common their negative impact on users' rights. Additionally, recent research by the Alliance for Affordable Internet showed that current zero rating programs did not bring most mobile internet users online for the first time, as many providers claim.[4] Rather, the vast majority of users prefer access to the full, global internet with time or data limitations, if restrictions must be imposed.

Recommendation: Design ICT policies and practices based on respect for human rights online and offline, upholding network neutrality, the rule of law, and protections against unlawful surveillance and censorship.

4. What are the elements of an enabling environment to build confidence and security in the use of the Internet?

Based on the 2015 OECD recommendations for digital security risk management, governments should focus on building out Digital Security across all sectors to promote user trust in the security of their devices and to empower the use of the internet to its fullest potential. Government and private entities need to consider user risk in establishing policy. This approach includes the measurable and concrete commitments put into action to secure the internet as a shared, global public resource and a gateway to the realization of human rights. It strives toward security measures that reinforce rather than undermine those rights.

Encryption tools, technologies, and services are essential to protect against harm and to shield our digital infrastructure and personal communications from unauthorized access. The ability to freely develop and use encryption provides the cornerstone for today's global economy.

Economic growth in the digital age is powered by the ability to trust and authenticate our interactions and communicate and conduct business securely, both within and across borders. Strong encryption and the secure tools and systems that rely on it are critical to improving cybersecurity, fostering the digital economy, and protecting users. Our continued ability to leverage the internet for global growth and prosperity and as a tool for organizers and activists requires the ability and the right to communicate privately and securely through trustworthy networks.

[4] http://a4ai.org/is-zero-rating-really-bringing-people-online/

The United Nations Special Rapporteur for freedom of expression has noted, “encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age.” As we move toward connecting the next billion users, restrictions on encryption in any country will likely have global impact. Encryption and other anonymizing tools and technologies enable lawyers, journalists, whistleblowers, and organizers to communicate freely across borders and to work to better their communities. It also assures users of the integrity of their data and authenticates individuals to companies, governments, and one another.

We encourage governments to support the safety and security of users by strengthening the integrity of communications and systems. All governments should reject laws, policies, or other mandates or practices, including secret agreements with companies, that limit access to or undermine encryption and other secure communications tools and technologies. Users should have the option to use – and companies the option to provide – the strongest encryption available, including end-to-end encryption, without fear that governments will compel access to the content, metadata, or encryption keys without due process and respect for human rights.

Recommendation: governments should promote and protect access to encryption and secure communications tools and technologies.

Specific security risks: Data Retention
One area where the security data is put at risk by governments is through “data retention mandates.” Data retention mandates pose significant challenges to the very foundations of the rule of law and international human rights, in particular to the right to privacy. Data retention compromises data security, exposing information to government and corporate misuse, data breaches, and employee theft. It also imposes significant costs, creates liability risks and negative externalities, and wastes energy at data centers. Ultimately these costs will be passed on to users.

The ITU should acknowledge the risk of data retention mandates for users’ privacy and its impact on data security. We realize that operators often need to retain specific information about their consumers, for instance for billing purposes. When determining data retention limits, the essential principles of necessity, proportionality, data minimisation and purpose limitations must be respected. Data minimisation establishes that information collected and processed should not be retained or further used unless this is necessary for clearly-indicated purposes. We instead recommend clear limits on data retention, preventing operators from retaining customer data longer than necessary for the legitimate purpose, without any caveat or exceptions.

Specific security risks: Deep Packet Inspection
Practices such as deep packet inspection (DPI) can have a severe impact on the right to privacy and must be carefully assessed. DPI techniques involve scanning the whole content of internet traffic. The scope of interference of these measures is increased due to the convergence of

communications through the internet, including those containing sensitive personal information.[5] The impact of data monitoring techniques such as DPI have often been compared to surveillance technologies and a link between the use of deep packet inspection and internet censorship have also been established by experts.[6] Given its broad and invasive power, use of DPI, and purchase and installation of DPI technology, must be strictly circumscribed.

5. What is the role of Governments in building an enabling environment?

Network Neutrality is a key guarantee in building an enabling environment on the internet. It means that all data traffic should be treated equally no matter its sender, recipient, type, or content. It also provides that all forms of discriminatory traffic management should be clearly prohibited. Network discrimination can happen at any level: applications, devices, protocols and even infrastructure connections deals. For this reason, laws and regulations need to be adopted by governments to avoid network discrimination that fails to meet the standard of narrowly targeted, temporary, necessary and transparent restrictions.

Network discrimination undermines human rights, such as the right to freely receive and impart information online. Net discrimination can also cause a barrier to competition and innovation online, e.g. by setting artificial advantages for certain content/market actors. This affects the equitable conditions that have fostered the dynamic and transformative nature of the internet since its creation.

After a long battle lasting several years from civil society and some corporate actors, the US Federal Communications Commission adopted what they call "strong rules to protect the internet". This constitutes a big advancement for Net Neutrality because the rules forbid paid prioritization (i.e. "fast lanes" for certain traffic), blocking, and throttling.

At least 47 countries have already enacted some kind of net neutrality legislation, since recently net neutrality was solidified in the European Union as a part of the Telecommunications Single Market (TSM) negotiations and subsequent development of implementation guidelines.

Strong legislation against activity which would harm Net Neutrality is essential in ensuring user access to the full, unfettered internet. This, in turn, ensures free speech and freedom of expression. Securing Net Neutrality is key, but governments must take far broader steps to

[5] European Data Protection Supervisor, EDPS Comments on DG Connect's Public Consultation on Specific Aspects of Transparency, Traffic Management and Switching in an Open Internet (Oct. 15, 2012), https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Comments/2012/12-10- 15%20_Open_Internet_EN.pdf

[6] Christopher Pasons, Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials (Jan. 10, 2009), http://christopher-parsons.com/Academic/WP_Deep_Packet_Inspection_Parsons_Jan_2009.pdf; Ralf, Bendrath, Governance of Deep Packet Inspection, (Feb. 15, 2009), http://userpage.fu-berlin.de/~bendrath/ISA09_Paper_Ralf%20Bendrath_DPI.pdf.

protect the rights of users online, including through regulatory enforcement of Net Neutrality legislation.

Recommendation: Pass and implement strong Network Neutrality regulation.

Data protection legislation and regulation is necessary to protect the right to privacy in the digital age. Data protection comprises a number of definitions and principles that empower individual users, or 'data subjects,' to control how their personal information is collected, processed, and transferred by third parties, whether corporate or public.

As noted in this European Digital Rights (EDRi) guide to data protection,[7] one of the most important principles is called purpose limitation. Purpose limitation is the principle that a data controller can only collect and use personal data for a specific purpose. This purpose must be properly defined and communicated to the person ("data subject") whose data are being processed. This permits the data subject to know what will happen to his/ her personal data. Under certain circumstances, a data controller may use personal data for a purpose other than the one for which the data were collected or provided in the first instance.

Without the principle of purpose limitation, a data controller could collect personal data for a certain purpose and continue to use it any way it wishes. The principle is therefore an important pillar to defend privacy, since it defines how much protection personal data receive once they have been collected by a controller. Weakening this principle would result in a major decrease of the protection of privacy of users. Yet it is just one of a basket of rights and principles that data protection legislation promotes and protects.

Many governments and bodies, including the European Union and the African Union, have convened to pass data protection conventions and mandates. Yet far too many countries either have not passed data protection legislation or consistently implemented their regulations. Filling these gaps in data protection law, and creating enabling environments through effective enforcement, will better protect privacy in the digital age, and promote fair and competitive practices by companies and governments in their respective roles.

Recommendation: pass and enforce data protection regulation.

Internet shutdowns are increasing worldwide. Access Now convened an international coalition to define and address this problem, creating the following definition: *An intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information*. Internet shutdowns occur when governments order companies to terminate or degrade public access to digital communications tools — like Twitter, SMS, or Facebook. Internet shutdowns threaten the open and accessible nature of the internet just as much as economically-motivated anti-competitive schemes, and must be strictly addressed by governments to ensure stable connections and an enabling environment for internet access.

[7] https://edri.org/files/paper06_datap.pdf

Even amidst times of conflict or events where public safety is threatened, internet shutdowns are a poor, blunt policy tool and must be avoided. Shutdowns do not help victims, restore order, or protect rights. Rather, they make things worse, by cutting off access to emergency services, reliable information, and crucial tools that families use to stay in touch with loved ones.

There have been more than 40 documented shutdowns in 2016, and dozens more over recent years on every continent. The problem has grown so dire that international institutions are pronouncing internet shutdowns a direct threat to human rights.

A growing body of jurisprudence declares shutdowns to violate international law. In 2015, experts from the United Nations (UN) Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), and the African Commission on Human and Peoples' Rights (ACHPR), issued an historic statement declaring that internet "kill switches" can never be justified under international human rights law, even in times of conflict. In 2016, the Human Rights Council referred to internet shutdowns in its consensus Resolution 32/13, which "condemns unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law, and calls upon all States to refrain from and cease such measures." Internet shutdowns are blanket bansthat are neither necessary nor proportionate, and therefore fail the test for restrictions on freedom of expression found in the Human Rights Committee's General Comment 34.

The internet has enabled significant advances in health, education, and creativity, and it is now essential to fully realize human rights including participation in elections and access to information. Shutdowns and blocking of internet services delay and deter the benefits of these advances and economic development more broadly, by obstructing trust in the digital economy, undermining access to information, and frustrating personal communications and resources needed for crisis response.

Recommendation: To create an enabling environment for internet access, governments must commit to not shutdown or throttle communications tools. Any officials or governments who do issue such orders must face immediate international condemnation and be held accountable by domestic and regional courts for the immediate and proximate harms the shutdowns cause.

For its part, the ITU should work with other international institutions, as well as national telecommunications regulators, to study the causes of internet shutdowns, identify and educate governments on rights-respecting alternatives, and increase accountability for the stability and resilience of networks against those who would obstruct it.

***

Access Now (www.accessnow.org) is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, global advocacy, and direct technical support, we fight for open and secure communications for all.

For more information, contact:
Peter Micek
Global Policy & Legal Counsel
Access Now | accessnow.org
peter@accessnow.org
+1-414-0100