DEMOCRATIC PRINCIPLES FOR AN OPEN INTERNET

Putting Open Internet Principles to Work for Democracy

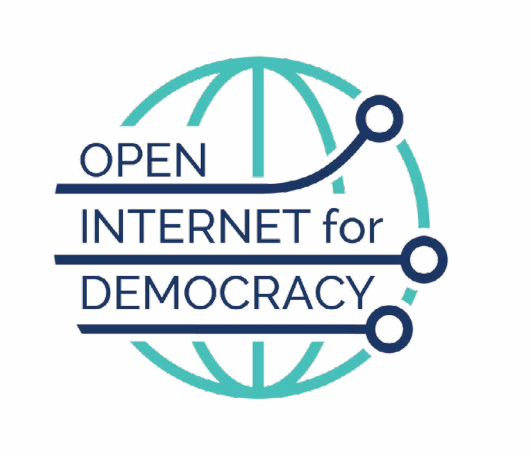

TABLE OF CONTENTS

OVERVIEW

An open internet – where all citizens can freely express themselves, share and debate ideas, and engage in economic activities – is an essential part of a modern, vibrant democracy. Ensuring that the internet remains both open and accessible is necessary to strengthen democratic engagement, enable equal participation in the market economy, and promote social accountability.

The increasing shift of political and social discourse to online platforms has led to a corresponding rise in the use of the internet as a tool that can silence dissent, promote violence, and perpetuate prevailing inequalities, including regarding access and use. The new and rapidly evolving nature of the internet means many citizens are unaware or misinformed as to how their fundamental rights such as to speech, assembly, and association apply in a digital world.

The Internet Rights and Principles Dynamic Coalition (IRPC) of the Internet Governance Forum (IGF) has developed a solid, sensible set of norms and standards based on the fundamental belief that all humans are born free and equal in dignity and rights, which must be respected, protected, and fulfilled in the online environment. Adherence to a universally applied set of standards and norms for a free and open internet that reflects a commitment to inclusion, participation, and accountability is a vital component of modern democracy. To create a framework for internet openness that advocates for more democratic societies based on the IRPC principles, the Center for International Private Enterprise (CIPE), the National Democratic Institute (NDI), and the Center for International Media Assistance (CIMA) have developed the Democratic Principles for an Open Internet.

As democratic citizens and reformers navigate changing political environments, we hope this guide will help activists working for democracy in an internet age and connect them in global peer networks to exchange best practices. The guide also serves as an advocacy tool that organizations can utilize in pushing governments, the private sector, and civil society to adhere to universal human rights through open internet principles and standards.

1. FREEDOM OF EXPRESSION

Everyone has the right to seek, receive, and impart information freely on the internet without censorship or other interference.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

The internet is a space for robust public debate where all people, regardless of religion, gender, ethnicity, sexual orientation, and socio-economic class can freely express their views, including dissenting opinions on policies, procedures, and/or public figures. Internet users have the right to debate any subject online without undue interference, illegal surveillance, or fear of retribution.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- Arbitrary blocking or filtering of content, such as the blocking of specific news media websites so that citizens cannot access relevant information.
- Abuse of defamation or intellectual property laws to stifle expression.
- Imposition of intermediary liability without adequate safe-harbour protections without adequate safe-harbour protections.
- Regulatory bodies and the judiciary request internet intermediaries such as internet service providers (ISPs), web hosting providers, website administrators, or social media platforms remove content without legal justification.
- Political actors disrupt democratic dialogue by flooding online spaces with disinformation, trolls, bots, or harassing language.
- Online violence, whether perpetrated by individuals or organizations causes politically-active citizens to self-censor or withdraw completely from public debate for fear of repercussions.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

In the *Philippines*, a cybercrime law introduced in 2012 proposed increasing penalties for libel and giving authorities unchecked power to track information online. Internet freedom activists worried several provisions of the law would infringe on freedom of expression by preventing Filipinos from freely posting content on websites, and participating in online forums and discussions without fear of being blocked or facing serious penalties. In response, pro-democracy organizations from across the political spectrum joined together to challenge the constitutionality of the law. Through protests, roundtables, and capacity building activities, they raised awareness and encouraged advocacy efforts around the dangers the law posted to freedom of expression and privacy. The Foundation for Media Alternatives (FMA), a digital rights organization founded after the fall of the Marcos dictatorship and the Philippine Internet Freedom Alliance (PIFA),

a broad nationwide coalition of pro-democracy and internet freedom advocates, were among the organizations in the front lines on the struggle. PIFA was even one of the 20 organizations to file 15 petitions to the Supreme Court about the constitutionality of the law.

Public efforts in the courts and actions in the streets contributed to the takedown of three contested provisions of the law, including provision that would allow government to block or restrict access to computer data. The Supreme Court declared these provisions unconstitutional and delayed implementation of the law. Despite public concerns about the surviving provisions, the national campaign against the cybercrime law led to a turning point for Filipino activists; it showed the power of people coming together and fighting for the importance of digital rights in the Philippines. Initially fragmented, the campaign led to a larger movement unified under the goal of protecting human rights and freedom of expression online. Thus, it took the introduction of a flawed law and active public campaigns to initiate a broader dialogue about privacy, surveillance, and digital security. Digital rights communities across Southeast Asia[1] have been inspired by Filipino advocacy efforts, which they have understood to be an example of how to communicate the balance required between anti-cybercrime measures with fundamental rights to a public audience.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- United Nations Declaration of Human Rights, Article 19: "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."[2]
- International Covenant on Civil and Political Rights, Article 19: "(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; (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." [3]
- United Nations Human Rights Council Resolution 32, 2016: "The same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."

[1] http://www.rstreet.org/2015/09/10/the-business-case-for-cambodian-Internet-freedom/

[2] http://www.un.org/en/universal-declaration-human-rights/

[3] http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

2. FREEDOM OF ASSEMBLY AND ASSOCIATION

Everyone has the right to associate freely through and on the internet for social, political, cultural or other purposes.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

The internet is an important platform for political organizing where citizens can collaborate to advance democratic goals. Citizens are able ato peacefully associate with others on the internet. The internet provides an open space for individuals to exercise their democratic rights and advocate for the rights of others.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- Citizens are prevented from accessing websites and messaging apps that facilitate political mobilization.
- Governments pressure websites and social media platforms to remove publicity for an event because it has the effect of limiting the ability of citizens to schedule a public meeting or organize a protest.
- Security agents infiltrate online communities to monitor groups.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

Social media is an important organizing tool for journalists and advocacy groups in *Uganda*. Facebook, WhatsApp, and other messaging applications have been used to share[4] political knowledge, connect leaders with supporters, and organize events — even share information about government abuses. During national 'Walk to Work'[5] protests in 2011, organized to protest living costs after presidential elections, Facebook and Twitter provided a steady stream of updates from protestors, bystanders, and journalists.

Using social media, however, can have dangerous consequences for marginalized groups such as the LGBT community. The government of Uganda has been known to collect user information and prosecute individuals based on information shared on social media. Uganda is one of 76 countries where homosexuality is currently criminalized, and LGBT activists fear that their online conversations will be monitored and used against them. By posting information

[4] https://books.google.com/books?id=2dmeBQAAQBAJ&pg=PA367

[5] https://en.wikipedia.org/wiki/Walk_to_work_protest

taken from photos and content posted on Facebook, a local tabloid exposed the identity of numerous members of the LGBT community in 2011 and again in 2014. The tabloid stories in 2011 are believed to have contributed to the killing of David Kato[6], a prominent gay rights activist.

Furthermore, the government has repeatedly restricted access for advocacy groups to use the internet to share political information. In 2016, the country's media regulator restricted the use[7] of WhatsApp, Facebook, and Twitter to prevent the organizing of protests before presidential elections in February as the government had done before in 2011. In both cases, the electoral commission enforced[8] the social media shut-down.

Civil society groups have responded in two ways. First, they have sought to deepen their digital security capacity. To protect against threats to journalists, LGBT organizations, and other groups have learned how to use Facebook and social media applications more securely and to implement other practices that increase their privacy. In the lead up to the 2016 election this included the use of virtual private networks (VPNs) to share information. Civil society groups spread information about how to use them through radio broadcasts. The fact that the hashtag #UgandaDecides trended on Twitter shows how they were able to spread their knowledge through local networks and connect with international media. Secondly, civil society groups built coalitions with international organizations to draw attention to abuses taking place in Uganda. In 2016, Access Now supported a coalition of groups to demand[9] that the government stop the internet shutdown as part of the #KeepitOn campaign.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- Article 20 of the UN Universal Declaration of Human Rights states that "Everyone has the right to freedom of peaceful assembly and association."
- Council of Europe's Human Rights for Internet Users, Assembly, Association and Participation. [10]"You have the freedom to choose any website, application or other service in order to form, join, mobilise and participate in social groups and assemblies whether or not they are formally recognised by public authorities."
- Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai, 21 May 2012. In the report, the Special Rapporteur calls upon States "to recognize that the rights to freedom of peaceful assembly and of association can be exercised through new technologies, including through the internet."

[6] https://www.theguardian.com/world/2016/jan/26/uganda-lgbt-groups-david-kato-murder-5-years-on

[7] http://www.bbc.com/news/world-africa-35601220

[8] https://freedomhouse.org/report/freedom-net/2016/uganda

[9] https://www.accessnow.org/uganda-blocks-social-media-harms-human-rights/

[10] http://www.coe.int/en/web/internet-users-rights/assembly-association-and-participation

3. ACCESSIBILITY

Everyone has an equal right to access and use a secure and open internet.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

All members of a society have an equal right to learn about, access, and use the internet. To ensure equal opportunity for participation, key public and private internet stakeholders identify and address existing inequalities in access, particularly among women and other marginalized populations.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- National broadband plans omit or unreasonably delay access to rural communities, leaving them with low bandwidth and/or high cost alternatives for online access.
- High costs prohibits access for poorer communities.
- Lack of investments in the infrastructure for broadband and mobile access throughout a country.
- Regulatory framework sometimes does not exist for market competition, etc.
- A government-mandated internet blackout in response to political protests compromises the earning power and income of local entrepreneurs who use the internet to conduct business.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

In *Nigeria*, national broadband plans have overlooked rural communities, leaving them with low bandwidth and high-cost options for internet access. This means that broadband and mobile data fees are unaffordable to many in Nigeria, especially the poor. Fixed-line broadband subscriptions cost an average of 39 percent of average income, and mobile broadband packages cost 13 percent. Given that approximately 80 percent of Nigerians earn below the poverty line ($2 a day or less), access to the internet is out of reach and unaffordable for a majority of citizens in Nigeria.

The Alliance for Affordable Internet, a global coalition working on Internet affordability, works with Nigerian civil society leaders to raise awareness around this issue through thematic working groups. The consumer advocacy and pricing transparency working group, for instance, works closely with a coalition of Nigerian NGOs [11]that have been leading campaigns to raise awareness about

[11] http://a4ai.org/a4ai-nigeria-multi-stakeholder-coalition/a4ai-nigeria-coalition-members/

pricing and taxation policies that have been proposed in Nigeria. One proposed policy includes imposing a nine percent tax on voice, data, and SMS services to consumers. This policy would make the internet dramatically more expensive for Nigerian consumers. Groups say they worry about the consequences of the proposed policy in an environment where farmers are forced to climb trees just to get a stable internet connection.

Civil society leaders who are part of the coalition have worked to build a healthy dialogue between regulators, civil society, and the government. A key strategy, according to activists, has been encouraging groups to find constructive ways to work with government and leveraging the interests of each of these groups to protect and drive down costs for Nigerian consumers. They seek to build relationships with the regulator and to inform them about ways to better communicate with and engage consumer groups, such as sharing their content through social media rather than press releases. Another important learning has been identifying champions within government to work on these issues.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- Council of Europe's Human Rights for Internet Users, Assembly, Association and Participation: "Your access should be affordable and non-discriminatory. You should have the greatest possible access to Internet content, applications and services using the devices of your choice."[12]

[12] http://www.coe.int/en/web/internet-users-rights/assembly-association-and-participation

4. PRIVACY AND DATA PROTECTION

Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

Security measures and online restrictions implemented by governments or other entities must be consistent with international human rights law and standards. Privacy and data protection also includes protection against unethical hacking, data interception, and identity theft. Internet intermediaries ensure adoption of policies and practices that protect against illegal requests for personal data by state or non-state entities.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- A government authority requiring that all computers sold in the country be equipped with filtering or surveillance software.
- Organizations that collect personal data from consumers do not ensure confidentiality and privacy of those data.
- Citizens are required to register their social media account usernames with the government so that they can easily track down and punish those who make anti-government statements.
- Governments criminalize encryption preventing citizens from safely corresponding with one another; journalists communicating with sources, and others.
- Government tracking all the activities and transactions of individuals using meta data analytics of citizen's identity card.
- Security and police forces requiring access to individual internet use by taking an individual's phone.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

In *Burma*, gaps in the law have left citizens vulnerable when it comes to privacy and data protection. Restrictions on privacy have eased since the country's transition from military rule, but a lack of data protection laws and general lack of awareness around privacy and data protection present significant challenges for protecting an open Internet. Messaging applications such as Viber and Facebook Messenger, for example, are the de-facto tool for communication for

activists and are used to organize political events and activities. Cheaper than voice calls, far more accessible than landlines, and easier to use than email, these tools are the primary way people in Burma communicate. Activists have received harsh penalties for sharing content that may be viewed as threatening state security[13]. These applications are often not secure, making it possible for Burma state authorities or agents of the state to intercept their conversations. During a crackdown on student protests in March 2015, mobile phones were taken by police[14]. Activists worried at the time that information on these phones would eventually be used against them.

Observing the need to protect activists and educate them about data protection, activists in 2016 formed a coalition, Digital Rights MM. The coalition, led by Phandeeyar, Myanmar Center for Responsible Business, Myanmar ICT for Development, and Free Expression Myanmar, has led a national conversation on the issue. Drawing on expertise from the region and international organizations[15], 22 local Burma-based organizations have been successful in pointing out gaps when it comes to privacy and freedom of expression in the national telecommunications law[16], a comprehensive law that oversees the development of the telecommunications sector in Burma. They also participated in meetings with the government and launched a public facing campaign #ourvoiceourhluttaw[17] pushing to amend 23 articles, including one on lawful interception of data.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- UN General Assembly, Resolution 69/166, Right to Privacy in the Digital Age 2014
- Standards for a Free, Open and Inclusive Internet, Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 2017
  - » *Paragraph 231*: Measures to restrict encryption reduce people's ability to protect themselves from illegal invasions of their privacy."
  - » *Paragraph 228:* "States have an obligation to respect anonymous discourse as an exercise of privacy and freedom of expression and may only exceptionally require authentication or proof of identity from the person expressing it, applying a standard of proportionality."
  - » *Paragraph 227*: "anonymous spaces that are free of observation and where identities and activities are not documented must be guaranteed."

[13] https://www.fastcompany.com/40438242/jailed-for-a-facebook-poem-the-fight-against-myanmars-draconian-defamation-law

[14] https://pen.org/sites/default/files/unfinished_freedom_lowres.pdf

[15] https://www.forbes.com/sites/chynes/2016/12/21/digital-rights-must-become-a-top-priority-in-myanmars-connectivity-revolution/#4fde153b2267

[16] https://www.article19.org/resources.php/resource/38665/en/myanmar:-telecommunications-law

[17] https://www.facebook.com/MMTelecomLaw/photos/a.821155664669495.1073741830.821091201342608/1347827635335626/?type=3&theater

» *Paragraph 212:* "Internet surveillance in any of its forms or nuances constitutes interference in the private lives of people and, when conducted illegally, can also affect the rights to due process and a fair trial, freedom of expression, and access to information. It is recognized both regionally and universally that illegal or arbitrary surveillance and interception and collection of personal data affect not only the right to privacy and freedom of expression but can also run contrary to the precepts of a democratic society"
» *Paragraph 204:* "To protect privacy on the internet, the confidentiality of personal online data must be guaranteed."

5. PERSONAL SAFETY AND SECURITY

The rights to personal safety and security must be respected, protected and fulfilled online. These rights must not be infringed upon, or used to infringe other rights, in the online environment.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

Legal protections are established that address threats of physical, sexual, and psychological violence or harassment made online. Furthermore, protections exist against online disinformation or trolling campaigns that incite violence, discrimination, or hostility against individuals or groups.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- Increasing reports from politically active women of online stalking, trolling, and blackmail generated in online spaces which have a gateway effect to in person and physical confrontation.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

In *Pakistan*, women face threats of physical, sexual, and psychological harassment online. Leaking explicit photos and threats of blackmail are growing increasingly more common. From 2014 to 2015, more than 3,000 cybercrimes were reported to the Federal Investigation Agency and of those cases, nearly half were targeted to women on social media[18]. Observers estimate far more cases go unreported. In fact, in workshops conducted by the The Digital Rights Foundation, many female college students reported that they did not know cyber harassment was a crime.

Online platforms are an important space for political engagement, expression, and mobilization in Pakistan. Thus, online harassment directly impacts the political participation of women, including female journalists and women politicians. In 2016 the Digital Rights Foundation established a Cyber Harassment Helpline[19] that women can reach out to for help when they are harassed on the internet. One of the main objective of the helpline is to help bridge the trust deficit between survivors and law enforcement agencies. An analysis of more than 400 cases[20] showed that the most common barriers to equal participation are non-consensual use of information, impersonation, account hacking, black

[18] https://digitalrightsfoundation.pk/drfpcwstraining/

[19] https://digitalrightsfoundation.pk/cyber-harassment-helpline-completes-its-four-months-of-operations/

[20] http://digitalrightsfoundation.pk/wp-content/uploads/2017/04/4-Month-Report.Final_.pdf

mailing, and receiving unsolicited messages; the most targeted groups include women, children, human rights defenders, and minority communities. The Digital Rights Foundation has also been leading efforts to strengthen legal protections for women and responding to survivors by recommendations to law enforcement agencies and the government. Pakistan has a National Response Centre for Cybercrime, but it has faced challenges serving women outside of major cities.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, paragraph 81: "States have an obligation to protect individuals against interference by third parties that undermines the enjoyment of the right to freedom of opinion and expression."

6. INCLUSION

Cultural and linguistic diversity on the internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

The internet is designed and maintained in a way that promotes inclusion of all peoples, such as women, persons with disabilities, and other marginalized populations. The content of the internet is created with a view towards promoting diversity and democratic participation. This includes linguistic diversity and adheres to accessibility standards, so that all individuals may communicate, share information, or create content online in the language of their choice.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- Official websites do not adhere to best practices or legal requirements for accessibility standards, preventing persons with disabilities from interacting with or using a site.
- Governments publishing information online routinely exclude translations for non-primary language-speaking members of the population.
- Online space becomes closed to the participation of women and marginalized peoples.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

In *India*, the population of people with disabilities is estimated to be as high as 150 million people, and the recorded rates of those who are vision-impaired are among the highest in the world. Indian digital rights advocacy groups, like the Centre for Internet and Society (CIS) have worked to ensure that these individuals are able to participate fully online by promoting policies that prioritize accessibility. These include the National Policy on Universal Electronics Accessibility, the Rights of Persons with Disabilities Act, and Guidelines for Indian Government Web (GIGW), which all require government information be shared in formats that are accessible. Advocacy groups, however, have successfully shown that policies alone are not enough and have taken action to ensure persons with disabilities have access to critical resources and information online.

Mobile phones in particular are a vital portal to access gover
nment services, but mobile applications remain largely inaccessible to many people with disabilities, especially those with vision disabilities. For example, CIS observed in 2015 that MyGov, the Indian Government's mobile citizen engagement platform and the Prime Minister's application was highly inaccessible: screens cannot be navigated by visually impaired users and can also not be read using a screen reader. Based on this, CIS with other advocacy organizations worked on framing accessibility guidelines for mobile applications recommended to the Government of India as a standard. Advocacy groups, such as the National Centre for Promotion of Employment for Disabled People (NCPEDP), have also been appealing to the private sector to ensure products designed to serve these needs are affordable and readily available to people with disabilities. They appeal to Indian companies and policymakers by advocating for the universal appeal of assistive technology to ensure disabled communities are not left behind.

Sustained advocacy, new legal mandates applied to public and private sectors, and increased research in this domain have helped advance the issue of accessibility of mobile applications. The country's National Informatics Centre has set up a committee to revise the GIGW to bring them up to speed with international standards.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, paragraph 87: "Where the infrastructure for internet access is present, the Special Rapporteur encourages States to support initiatives to ensure that online information can be accessed in a meaningful way by all sectors of the population, including persons with disabilities and persons belonging to linguistic minorities."
- Standards for a Free, Open and Inclusive Internet, Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 2017[21] "States should take measures designed to reduce linguistic obstacles in order to make literacy viable and ensure access for all people under equal conditions. They should also "promote original local and indigenous content on the internet."

[21] http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf

7. NETWORK EQUALITY

Everyone shall have universal and open access to the internet's content, free from discriminatory prioritisation, filtering or traffic control on commercial, political or other grounds.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

All citizens have equal access to publicly available content on the internet. The sites and services citizens are able to access are not discriminated against based on their political content. Shutting down or throttling access to the internet is not permitted on any grounds, including public order or national security grounds.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- Speeding up of specific content in exchange for commercial considerations.
- An internet blackout that cuts off access in a given country, region, city, or neighborhood.
- The throttling of internet service during elections or other political event (e.g. protests) so that images or videos cannot be circulated by citizens.
- A citizen in one country is unable to access websites that are widely available in other countries due to local government censorship and regulation.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

A government-enforced internet shutdown in C*ameroon* denied online access to a significant portion of the country's population for more than three months in early 2017[22]. The shutdown targeted the Anglophone region of the country, an area historically marginalized by the French-speaking majority. In the lead up to the internet blackout, the Cameroonian government publicly warned internet users there would be criminal penalties for any actions to spread false news on social media in the Anglophone region. Despite the government's claim that this action would prevent the spread of false information, most observers held that the government aimed to stem recent protests by limiting connections to social media messaging applications and other online communication platforms. Activists believe the government was acutely aware of the critical role the internet played in organizing protests.

[22] http://www.bbc.com/news/world-africa-39665244

Digital rights groups unaffected by the shutdown launched a global social media campaign, #bringbackourinternet, to raise awareness about the shutdown. They sought to lead efforts to apply local, pan-African and international pressure on the government. They also directly engaged Camtel, the country's national telecommunications company. Finally, startups created an "internet refugee camp,"[23] where members brought portable internet modems for others to use instead of driving to the next largest city, Douala, to use the internet. Through these efforts, the Cameroonian technology and activist communities raised global awareness about the shutdown, applying pressure on the government.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, paragraph 79: "The Special Rapporteur calls upon all States to ensure that internet access is maintained at all times, including during times of political unrest."[24]

[23] https://qz.com/942879/an-internet-shutdown-in-cameroon-has-forced-startups-to-create-an-internet-refugee-camp-in-bonako-village/

[24] http://www.un.org/ga/search/view_doc.asp?symbol=A/HRC/17/27

8. STANDARDS

The internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion and equal opportunity for all.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

Internet standards/formats should be open with little to no barriers to access ensure users, content hosts, and service providers are able to freely exchange information. Technical standards are not used as a way to accomplish censorship or surveillance.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- A technical standard is developed with the express intent of enabling tracking or surveillance of individual internet users.
- A government refuses to adopt international internet standards effectively limiting citizens' access to the global internet.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

Communicating safely and securely online is a challenge for democracy activists and journalists *everywhere*. In the last ten years, global advocacy groups Center for Democracy and Technology (CDT) and the Electronic Frontier Foundation (EFF) have called on website owners to support HTTPS, or Hypertext Transfer Protocol with an additional S for "secure."

Using an HTTPS site helps ensure that users connect to the sites they intend to, and that content transferred between the website server and a user's browser is less susceptible to surveillance or interference. The extra layer of security makes it less likely for government agents, internet service providers, or hackers to surveil users online. Without HTTPS, an agent could replace news stories or Wikipedia entries with alternative content, track readers' habits, and even intercept passwords.

Since the original HTTPS protocol was released in 1995, it has become an industry standard for offering encryption and content authentication on the internet. In 2010, Google modified its search engine to make browsers send search queries through HTTPS[25] and Wikipedia and Facebook

[25] https://web.archive.org/web/20100526165218/http:/www.h-online.com:80/security/news/item/Google-secures-search-with-SSL-encryption-1006020.html

also later adopted HTTPs by default[26]. Media organizations such as the BBC, Washington Post, and The New York Times have also migrated to HTTPS. Today, the average volume of encrypted traffic surpasses unencrypted traffic[27].

Despite greater awareness, there is more to be done, says the Freedom of the Press Foundation, pointing out that several major international news sites have not yet migrated their sites to HTTPS, including Al Jazeera, El Mundo (Spain), France 24 (France), Xinhua News Agency (China), and The Hindu (India). Through global advocacy campaigns, CDT and EFF have also educated industry players on the benefits of HTTPS. Migration tools such as Let's Encrypt, a service developed by the Internet Security Research Group, and EFF's browser plug-in, HTTPS://everywhere, support the needs of smaller site owners and users. Importantly, these groups view having segmented advocacy strategies for stakeholder groups, including tailored messages, as an important strategy to furthering awareness and action.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- Standards for a Free, Open and Inclusive Internet, Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, 2017 - Paragraph 231: "Measures to restrict encryption reduce people's ability to protect themselves from illegal invasions of their privacy. The measures include… the imposition of centralized key registries or the creation of back doors to enable collection of communication even from encrypted devices."[28]
- OECD Council Recommendation on Principles for Internet Policy Making. December 2013. "The internet allows people to give voice to their democratic aspirations and that any policy-making associated with it must promote openness and be grounded in respect for human rights and the rule of law" [29]

[26] https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920/

[27] https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/

[28] http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf

[29] http://www.oecd.org/sti/ieconomy/49258588.pdf

9. GOVERNANCE

Human rights and social justice must form the legal and normative foundations upon which the internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation and accountability.

WHAT DOES THIS LOOK LIKE IN A DEMOCRACY?

The stakeholders involved in internet governance represent a cross-sector of organizations, such as governments, civil society groups, private sector representatives, academia, and the media in order to truly be democratic and pluralistic. Diversity is essential to making sure that internet governance is inclusive and representative.

WARNING SIGNS OF AN UNDEMOCRATIC INTERNET:

- Internet governance bodies include only government and government-appointed representatives.
- Internet governance conferences and forums either directly or indirectly exclude participation from Global South representatives.
- Only multinational technology and telecommunication companies are present, excluding other large portions of the private sector, such as entrepreneurs or small business associations.

SUCCESSFUL ADVOCACY EFFORTS TO DEFEND THIS PRINCIPLE:

In *Nepal,* the national chapter of the Internet Society has led efforts to create a national multi-stakeholder governance structure that includes government, civil society, and the private sector by organizing a national Internet Governance Forum. In so doing, they have sought to ensure decisions about internet policy include the participation of all the stakeholders affected.

In 2009, Shreedeep Rayamajhi and a group of activists launched the Internet Society chapter in Nepal. After attending the global Internet Governance Forums (IGF), a multi-stakeholder policy conference organized under the auspices of the United Nations, the Nepalese digital rights activists decided to plan their own IGF in Nepal. This took place in the context where abuse of citizen rights online mounted and awareness about the lack of specific laws and regulations to protect them grew. There was a growing sense among civil society groups that a new platform needed to be developed to discuss these issues.
Through IGF Nepal meeting and the work of the Nepalese Internet Society chapter, these activists are able to provide platforms for people,

particularly youth, to discuss their vision and strategies for fostering a more open and safe internet in Nepal and share these ideas with global policymakers. Importantly, they view it as the beginning of a larger effort to develop a mechanism for engaging the domestic and international policymaking community, which still has a developing level of understanding around how internet governance issues are understood and implemented in the Global South.

SELECTED SOURCES FROM INTERNATIONAL FRAMEWORKS:

- WSIS Declaration of Principles. 12 December 2003. Article 20. "Governments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires cooperation and partnership among all stakeholders."[30]
- OECD Council Recommendation on Principles for Internet Policy Making. 13 December 2011.[31]

[30] http://www.itu.int/net/wsis/docs/geneva/official/dop.html

[31] http://www.oecd.org/sti/ieconomy/49258588.pdf

HTTPS://OPENINTERNET.GLOBAL

National Endowment
for Democracy
Supporting freedom around the world