

Module 3

**ACCESS TO
THE
INTERNET**

*Summary Modules on
Litigating Digital Rights
and Freedom of
Expression Online*



**MEDIA
DEFENCE**

Published by Media Defence: www.mediadefence.org
This module was prepared with the assistance of ALT Advisory: <https://altadvisory.africa/>

Originally published in December 2020
Revised in November 2022

This work is licenced under the Creative Commons Attribution-NonCommercial 4.0 International License. This means that you are free to share and adapt this work so long as you give appropriate credit, provide a link to the license, and indicate if changes were made. Any such sharing or adaptation must be for non-commercial purposes and must be made available under the same “share alike” terms. Full licence terms can be found at <https://creativecommons.org/licenses/by-ncsa/4.0/legalcode>.



TABLE OF CONTENTS

IS THERE A RIGHT TO THE INTERNET UNDER INTERNATIONAL LAW?	1
INTERFERENCES WITH ACCESS TO THE INTERNET	5
WHAT IS AN INTERNET SHUTDOWN?	6
WHAT IS THE BLOCKING AND FILTERING OF CONTENT?	7
WHAT IS NETWORK NEUTRALITY?	8
LIMITATION OF THE RIGHT TO FREEDOM OF EXPRESSION	9
NATIONAL SECURITY AS A GROUND OF JUSTIFICATION	11
INTERMEDIARY LIABILITY	13
CONCLUSION.....	17

MODULE 3

ACCESS TO THE INTERNET

- An express right to the internet has not been recognised in international law. However, it is widely accepted that access to the internet enables a variety of other fundamental rights.
- Practices such as internet shutdowns and blocking and filtering of content often violate the rights to freedom of expression and have rarely been found to constitute a justifiable limitation.
- National security is frequently relied upon as the justification for an interference with access to the internet, as well as other interferences with the right to freedom of expression. While national security is listed as one of the legitimate aims for derogation from the right to freedom of expression in appropriate circumstances, it is often used by states to quell dissent and cover up state abuses.
- ‘Net neutrality’ refers to the principle that all internet data should be treated equally without undue interference, and the concept promotes the widest possible access to information on the internet.
- Intermediary liability occurs when governments or private litigants can hold technological intermediaries, such as internet service providers (ISPs) and websites, liable for unlawful or harmful content created by users of those services. Such liability has a chilling effect on freedom of expression online.

IS THERE A RIGHT TO THE INTERNET UNDER INTERNATIONAL LAW?

An express right to the internet has not yet been recognised in any international treaty or similar instrument. This has been the source of much debate, and the arguments for and against the right of access to the internet are numerous.

Arguments in favour of access to the internet as a human right¹	Arguments against access to the internet as a human right
<ul style="list-style-type: none"> • Necessity. There is consensus not only on the usefulness of the internet but its crucial role as an “indispensable tool” for human rights and development in the current century. • Implied existence under current international human rights law. The full exercise of freedom of expression, participation in cultural life, and enjoyment of scientific benefits requires access to the internet. Current standards of living include participation in the broader community in different ways, e.g. through the connection to the internet. • Inevitability. Several countries including Greece, Estonia, Finland, Spain, Costa Rica, and France, have asserted or recognised some right of access in their constitutions, legal codes, or judicial rulings, and courts in Africa are increasingly finding that access to the internet is a corollary of the right to freedom of expression. • Inseparability. Technological progress changes how people enjoy their rights and governments should address the link between those rights and their current methods of enjoyment. 	<ul style="list-style-type: none"> • No international treaty directly creates a right of access to the internet, although some countries, mostly in Europe, have domestic legislation that does.³ In simple terms, it is not a human right if the international community has not recognised it as such in a binding instrument, and there is presently no new treaty under discussion to do so. • Analogy to other forms of media. There is no right to the telephone, the television, the printed press (either for publishing or receiving) or any other similar medium that has imposed a duty on states to provide it to citizens and cover its costs. • Universality. Access to the internet is not an economic right that can be construed from article 11 of the ICESCR and article 25 of the UDHR, for they are representative of standards of living that cannot be considered on the same scale for countries in much different stages of development. • Nature as a right. Even if there is a legal consideration of access, it is established not as much as an individual right but as an obligation for states. • Means to an end. Access to the internet consists of technology, which is a tool, not a right itself.

¹ Juan Carlos Lara, ‘Internet access and economic, social and cultural rights’, Association for Progressive Communications (September 2015) at p 10-11 (accessible at: https://www.apc.org/sites/default/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29_0.pdf). See, also, The 2019 Report of the UN Secretary-General’s High level panel on Digital Cooperation noted that “universal human rights apply equally online as offline – freedom of expression and assembly, for example, are no less important in cyberspace than in cyberspace than in the town square” at p 16 (accessible at: <https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf>). In *Delfi v Estonia* the European Court of Human Rights held that the internet provided an unprecedented platform for the exercise of the right to freedom of expression (accessible at: <https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/>).

³ For more, see here: <https://www.promisehumanrights.blog/blog/2021/10/the-human-right-to-internet-access>.

- **Progression.** The notion of rights themselves has the ability to change as social contexts change. The growing importance of the internet in changing social contexts makes it necessary to ensure access.
- **Public support.** Worldwide surveys show a single predominant attitude towards access to the internet: that it should be recognised as a right.²
- **Negative duty.** While there is not currently a positive duty on states to provide access to the internet, there is increasing jurisprudence holding that states have a negative duty not to interfere with access.
- **Access to the internet is not absolutely necessary for participation in a political community.** A big part of the world's population is without internet access. It is only when such participation already exists and is taken away that it gets attention.
- **Inflation.** Claiming that an interest is a basic, fundamental or human right, without considering the conditions under which it can really be realised, inflates the number of rights, diminishing the forcefulness of core traditional human rights.
- **Flexibility of existing human rights.** It is not necessary to create new rights aside from those already recognised but to ensure their exercise and enjoyment in changing technological contexts.
- **Side effects.** Digital inclusion policies carry concerns regarding the true beneficiary. On one hand, access policies will benefit those users with devices and the ability to access the internet, therefore exacerbating inequalities. On the other hand, lack of control by governments could lead to the need for investment in private telecommunications companies, therefore granting them economic benefit before citizens.

There is an increasing recognition of access to the internet being indispensable to the enjoyment of an array of fundamental rights. The corollary is that those without access to the internet are deprived of the full enjoyment of those rights, which, in many instances, can exacerbate already existing socio-economic divisions. For instance, a lack of access to the internet can impede an individual's ability to obtain key information, facilitate trade, search for jobs, or consume goods and services.

Access entails two distinct but interrelated dimensions: (i) the ability to see and disseminate content online; and (ii) the ability to use the physical infrastructure to enable access to such

² The Internet Society, 'Global Internet User Survey 2012' (2012) (accessible at: <https://wayback.archive-it.org/9367/20170907075228/https://www.internetsociety.org/sites/default/files/rep-GIUS2012global-201211-en.pdf>).

online content. In 2003, UNESCO was among the first international bodies to call on states to take steps to realise a right of access to the internet. In this regard, it stated that:⁴

“Member States and international organizations should promote access to the Internet as a service of public interest through the adoption of appropriate policies in order to enhance the process of empowering citizenship and civil society, and by encouraging proper implementation of, and support to, such policies in developing countries, with due consideration of the needs of rural communities.

...

Member States should recognize and enact the right of universal online access to public and government-held records including information relevant for citizens in a modern democratic society, giving due account to confidentiality, privacy and national security concerns, as well as to intellectual property rights to the extent that they apply to the use of such information. International organizations should recognize and promulgate the right for each State to have access to essential data relating to its social or economic situation.”

In 2012, the United Nations Human Rights Council (**UNHRC**) passed an important resolution that “[called] upon all States to facilitate access to the Internet and international cooperation aimed at the development of media and information communications facilities in all countries.”⁵

This has been expanded upon in the United Nations Sustainable Development Goals (**SDGs**), which recognise that “[t]he spread of information and communications technology and global interconnectedness has great potential to accelerate human progress, to bridge the digital divide and to develop knowledge societies.”⁶ The SDGs further call on states to enhance the use of Information Communication Technologies (**ICTs**) and other enabling technologies to promote the empowerment of women,⁷ and to strive to provide universal and affordable access to the internet in least developed countries by 2020.⁸

The 2016 UN Resolution on the Internet, adopted by the UN Human Rights Council, recognises that the internet can accelerate progress towards development, including in achieving the SDGs, and affirms the importance of applying a rights-based approach in

⁴ UNESCO, ‘Recommendation concerning the promotion and use of multilingualism and universal access to cyberspace’ at paras 7 and 15 (accessible at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Eng%20-%20Recommendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf).

⁵ UNHRC, ‘Resolution on the promotion, protection and enjoyment of human rights on the internet’, A/HRC/20/L.13, 29 June 2012 at para 2 (accessible at: https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc). This was expanded upon further the following year in UNHRC, ‘Resolution on the promotion, protection and enjoyment of human rights on the internet’, A/HRC/Res/26/13, 14 July 2014 (accessible at: https://hrlibrary.umn.edu/hrcouncil_res26-13.pdf).

⁶ UNGA, ‘Transforming our world: The 2030 agenda for sustainable development’, A/Res/70/1, 21 October 2015 at para 15 (accessible at https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E).

⁷ *Id.* at goal 5(b) at p 18.

⁸ *Id.* at goal 9(c) at p21.

providing and expanding access to the internet.⁹ Notably, it affirms the importance of applying a comprehensive rights-based approach in providing and expanding access to the internet¹⁰ and calls on states to consider formulating and adopting national internet-related public policies with the objective of universal access and the enjoyment of human rights at their core.¹¹

Notwithstanding whether the internet is seen as a self-standing right or an enabling tool to facilitate the realisation of other rights, the groundwork has been firmly laid for the need to realise universal access to the internet. States are concomitantly required to take steps to achieve universal access. However, in reality, universal access to the internet is far from being realised. This is due to a confluence of factors, including a lack of financial resources at both the individual and state levels, inadequate locally-relevant content, insufficient levels of digital literacy, and a lack of political will to make this a priority.

INTERFERENCES WITH ACCESS TO THE INTERNET

Some of the ways in which access to the internet is interfered with are through internet shutdowns, the disruption of online networks and social media sites, and the blocking and filtering of content. Such interferences can pose severe restrictions on the enjoyment of the right to freedom of expression, as well as the enjoyment of a range of other rights and services (including mobile banking, access to education, online trade, and the ability to access government services via the internet).

The act of disrupting or blocking access to internet services and websites amounts to a form of prior restraint. Prior restraints are State actions that prohibit speech or other forms of expression before they can take place.¹² Due to the profound chilling effect prior restraint can have on the exercise of the right to freedom of expression, the International Covenant on Civil and Political Rights ([ICCPR](#)) has been interpreted as providing for an effective prohibition on most forms of prior restraint on speech.¹³ The American Convention on Human Rights contains a similar prohibition.¹⁴ It is therefore imperative that, in order for any such measure

⁹ UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', A/HRC/Res/32/13, 18 July 2016 at para 2 (accessible at: <https://www.refworld.org/docid/57e916464.html>).

¹⁰ *Id.* at para 5.

¹¹ *Id.* at para 12.

¹² Council of Europe, 'Prior Restraints and Freedom Of Expression: The Necessity of Embedding Procedural Safeguards in Domestic System' (May 2018), (accessible at: <https://rm.coe.int/factsheet-prior-restraints-rev25may2018/16808ae88c>).

¹³ This has been inferred from the *travaux préparatoires* of the ICCPR that prior restraints are absolutely prohibited under article 19 of the ICCPR. See Marc J. Bossuyt, 'Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights', Martinus Nijhoff (1987) at p 398.

¹⁴ Article 13: "1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice. 2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: a. respect for the rights or reputations of others; or b. the protection of national security, public order, or public health or morals."

to be permissible, it must be able to comply with the three-part limitations test detailed in Module 1.

WHAT IS AN INTERNET SHUTDOWN?

An internet shutdown may be defined as 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.¹⁵ In other words, this arises when someone, be it the government or a private sector actor, intentionally disrupts the internet, a telecommunications network or an internet service, arguably to control or curb what people say or do.¹⁶ This is sometimes also referred to as a ‘kill switch.’

In some instances, this may entail there being a total network outage, whereby access to the internet is shut down in its entirety. In others, it may be access to mobile communications, websites, or social media and messaging applications that is blocked, throttled, or rendered effectively unusable.¹⁷ Shutdowns may affect an entire country, specific towns or regions within a country, or even multiple countries, and have been seen to range from several hours to several months.¹⁸

It should be noted that in order to conduct shutdowns, governments typically require the action of private actors that operate networks or facilitate network traffic.¹⁹ As noted by the United Nations Special Rapporteur (UNSR) on freedom of expression, large-scale attacks on network infrastructure committed by private parties, such as distributed denial-of-service (known as ‘DDoS’) attacks, may also have shutdown effects.

ECOWAS Court finds internet shutdowns illegal

In a landmark case confirming that internet shutdowns constitute a form of prior restraint and an unjustifiable infringement on freedom of expression, in June 2020, the Economic Community of West African States (**ECOWAS**) Community Court of Justice (**ECOWAS Court**) ruled that the internet shutdowns implemented by the Togolese government in 2017 were illegal.²⁰ In the judgment, *Amnesty International Togo v the Togolese Republic*, the court held that access to the internet is a “derivative right” as it “enhances the exercise of freedom of expression” and as such is “a right that requires protection of the law.”²¹

¹⁵ Access Now, ‘What is an internet shutdown?’ (accessible at: <https://www.accessnow.org/keepiton/?ignorelocale>).

¹⁶ *Id.*

¹⁷ Report of the UNSR on Freedom of Expression to the UNGA, A/HRC/35/22, 30 March 2017 (2017 Report of the UNSR on freedom of expression) at para 8 (accessible at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement>).

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ ECOWAS Community Court of Justice, Suit No. ECW/CCJ/APP/61/18 (2020) (accessible at: http://prod.courtecowas.org/wp-content/uploads/2020/09/JUD_ECW_CCJ_JUD_09_20.pdf).

²¹ Amnesty International Togo v The Togolese Republic (2020) (accessible at: <https://globalfreedomofexpression.columbia.edu/cases/amnesty-international-togo-and-ors-v-the-togolese-republic/>.)

In a similar case in 2022 relating to the blocking of specific content, rather than a wholesale internet shutdown, the ECOWAS Court considered the government of Nigeria's banning of social media platform Twitter, underscoring that modern technology has enabled the exchanges of ideas, views, and opinions and thus furthers freedom of expression, and held that access to Twitter is a "derivative right" that is "complementary to the enjoyment of the right to freedom of expression."²²

WHAT IS THE BLOCKING AND FILTERING OF CONTENT?

Although a less drastic measure than a complete internet shutdown, the blocking and filtering of content online can also hinder the full enjoyment of the right to freedom of expression.

Blocking/filtering has been defined as follows:

- "[T]he difference between "filtering" and "blocking" is a matter of scale and perspective.
- Filtering is commonly associated with the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or on the basis of their perceived connection to content deemed inappropriate or unlawful;
 - Blocking, by contrast, usually refers to preventing access to specific websites, domains, IP addresses, protocols or services included on a blacklist."²³

For example, in March 2020 social media sites were blocked in Guinea during a referendum;²⁴ and in October that same year, a general shutdown of the internet ensued during the General Election.²⁵ Even after the general connection was re-established, users reported that certain sites, specifically Facebook, remained blocked for a few more weeks. Guinea is unfortunately far from the only African country to implement such techniques in recent years.²⁶ In 2018, after an extensive period of blocking a long list of websites, including media outlets and prominent websites known for their reporting on protests in the country, the Ethiopian government unblocked 264 websites, although instances of blocking of social media occurred again in 2022.²⁷

²² SERAP v. Federal Republic of Nigeria (2022) (accessible at: <https://globalfreedomofexpression.columbia.edu/cases/serap-v-federal-republic-of-nigeria/>.)

²³ ARTICLE 19, 'Freedom of expression unfiltered: How blocking and filtering affect free speech, October 2016 at p 7 (accessible at: https://www.article19.org/data/files/medialibrary/38588/Blocking_and_filtering_final.pdf).

²⁴ Access Now, 'A broken promise to #KeepItOn: Guinea cuts internet access and blocks social media on referendum day' (2020) (accessible at: <https://www.accessnow.org/a-broken-promise-to-keepit-on-guinea-cuts-internet-access-and-blocks-social-media-on-referendum-day/>).

²⁵ Access Now, 'How internet shutdowns are threatening 2020 elections, and what you can do about it' (2020) (accessible at: <https://www.accessnow.org/internet-shutdowns-2020-elections/>).

²⁶ BBC, 'Africa internet: Where and how are governments blocking it?' (2020) (accessible at: <https://www.bbc.com/news/world-africa-47734843>).

²⁷ Freedom on the Net, 'Ethiopia' (2022) (accessible at: <https://freedomhouse.org/country/ethiopia/freedom-net/2022>.)

WHAT IS NETWORK NEUTRALITY?

Network neutrality — or “net neutrality” — refers to the principle that all internet data should be treated equally without undue interference, and promotes the widest possible access to information on the internet.²⁸ In other words, it promotes the idea that ISPs should treat all data that travels over their networks fairly, without improper discrimination in favour of a particular application, website, or service.²⁹ Discrimination in this regard may relate to halting, slowing or otherwise tampering with the transfer of any data, except for a legitimate network management purpose, such as easing congestion or blocking spam.³⁰

The 2017 Report of the UNSR on freedom of expression describes two key ways in which net neutrality may be compromised:³¹

- **Paid prioritisation schemes** — where providers give preferential treatment to certain types of internet traffic over others for payment or other commercial benefit.
- **Zero-rating** — which is the practice of not charging for the use of internet data associated with a particular application or service, while other services or applications are subject to metered cost.

In various countries around Africa, there has been significant debate about access to zero-rated content, particularly as social networking sites have begun to offer some measure of free access to users. On the one hand, zero-rating provides access to persons who might not otherwise have been able to access the internet and can provide critical free information on topics of public importance. For example, zero-rating was used extensively during the COVID-19 pandemic in South Africa to enable wider access to public health information about the disease and its prevention.³² On the other hand, critics argue that zero-rating can lead to unfair competition and distort users’ perceptions by only allowing access to particular sites, thereby limiting access to information.³³

The [2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa](#) protects network neutrality by calling on states to require internet intermediaries to enable access to all internet traffic equally and not to interfere with the free flow of information by giving preference to particular internet traffic.³⁴

²⁸ 2017 Report of the UNSR on freedom of expression above at n 18 at para 23.

²⁹ Electronic Frontier Foundation, ‘Net neutrality’ (accessible at: <https://www.eff.org/issues/net-neutrality>).

³⁰ American Civil Liberties Union, ‘What is net neutrality?’ (accessible at: <https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality>).

³¹ 2017 Report of the UNSR on freedom of expression above n 18 at paras 24-28.

³² ISPA, ‘Press Release : ISPA Helps Consumers Verify Zero-Rated Websites in SA,’ (2020) (accessible at: https://ispa.org.za/press_releases/ispa-helps-consumers-verify-zero-rated-websites/).

³³ For a discussion on zero-rating in Africa, see Research ICT Africa, ‘Much ado about nothing? Zero-rating in the African context’, 12 September 2016 (accessible at: https://www.researchictafrica.net/publications/Other_publications/2016_RIA_Zero-Rating_Policy_Paper_-_Much_ado_about_nothing.pdf).

³⁴ Principle 39.

LIMITATION OF THE RIGHT TO FREEDOM OF EXPRESSION

In 2016, the UNSR on freedom of expression noted that “[t]he blocking of Internet platforms and the shutting down of telecommunications infrastructure are persistent threats, for even if they are premised on national security or public order, they tend to block the communications of often millions of individuals”.³⁵ This poses an obvious limitation on the right to freedom of expression and may further limit a range of other rights.

The 2011 Joint Declaration on Freedom of Expression and the Internet highlights the egregious nature of these limitations:³⁶

- “(a) Mandatory blocking of entire websites, [internet protocol (IP)] addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse.
- (b) Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression.
- (c) Products designed to facilitate end-user filtering should be required to be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.”

Internet and telecommunications shutdowns that involve measures to intentionally prevent or disrupt access to or dissemination of information online are a violation of human rights law.³⁷ In the 2016 UN Resolution on the Internet, the UN Human Rights Council stated that it “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”.³⁸

As set out in General Comment No. 34:³⁹

“Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with [article 19(3) of the ICCPR]. Permissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with [article 19(3) of the ICCPR]. It is also inconsistent with [article 19(3) of the ICCPR] to prohibit a site or an information

³⁵ Report of the UNSR on Freedom of Expression to the UNGA, A/71/373, 6 September 2016 (2016 Report of the UNSR on Freedom of Expression) at para 22 (accessible at: https://www.un.org/ga/search/view_doc.asp?symbol=A/71/373).

³⁶ International Mechanisms for Promoting Freedom of Expression, ‘Joint declaration on freedom of expression and the internet’, 1 June 2011 (2011 Joint Declaration).

³⁷ 2017 Report of the UNSR on freedom of expression above n 18 at para 8.

³⁸ 2016 UN Resolution on the Internet above n 8 at para 10.

³⁹ General Comment No. 34 at para 43.

dissemination system from publishing material solely on the basis that it may be critical of the government or the political social system espoused by the government.”

The 2019 [Declaration of Principles on Freedom of Expression and Access to Information in Africa](#) also calls on states not to condone or engage in any disruption of access to the internet or other digital technologies, and not to interfere with the rights to freedom of expression and access to information “through measures such as the removal, blocking or filtering of content, unless such interference is justifiable and compatible with international human rights law and standards.”⁴⁰

The UNSR on freedom of expression has noted that internet shutdowns are often ordered covertly and without a legal basis, and violate the requirement that the restrictions must be provided for in law.⁴¹ Similarly, shutdowns ordered pursuant to vaguely formulated laws and regulations, or laws and regulations that are adopted and implemented in secret, also fail to satisfy the legality requirement.⁴² In some countries, this has led to the government enacting new laws to expressly allow for shutdowns to take place.⁴³

The UNSR on Freedom of Expression has further noted that network shutdowns invariably fail to meet the standard of necessity,⁴⁴ and are generally disproportionate.⁴⁵ States frequently seek to justify this on the ground of national security, which is discussed further below. For example, Chad blocked social media for a period of 472 days in 2018,⁴⁶ ostensibly for security reasons. A case was filed against two internet providers,⁴⁷ but access was restored shortly after.

⁴⁰ Principle 38.

⁴¹ 2017 Report of the UNSR on Freedom of Expression at para 9.

⁴² *Id.* at para 10.

⁴³ In India, for example, following the internet reportedly having been shut down more than 40 times during the course of 2017, the Department of Telecommunications issued new rules - the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules - in August 2017 allowing the government to shut down telephone and internet services during a public emergency or for public safety. The government had previously relied on section 144 of the Criminal Code that was aimed at preventing “obstruction, annoyance or injury” to impose internet restrictions. This legal development has been met with mixed responses. On the one hand, the new rules would potentially mean that, if the government were to persist with internet shutdowns, this could arguably be done in a more organised manner. On the other hand, however, concerns have been raised about the lack of definitions for the terms “public emergency” or “public safety”, and the potential that these new rules may have for censorship online. See: for instance, <http://www.hindustantimes.com/india-news/govt-issues-first-ever-rules-to-carry-out-internet-shutdowns-in-india/story-Drn0MnxJAp58RoZoF17u4L.html>.)

⁴⁴ 2017 Report of the UNSR on freedom of expression above n 18 at para 14.

⁴⁵ *Id.* at para 15.

⁴⁶ Quartz Africa, ‘Chad has now spent a full year without access to social media’ (2019) (accessible at: <https://qz.com/africa/1582696/chad-has-blocked-whatsapp-facebook-twitter-for-a-year/>).

⁴⁷ Africa News, ‘Chadian lawyers challenge ongoing social media shutdown’ (2018) (accessible at: <https://www.africanews.com/2018/08/21/chadian-lawyers-challenge-ongoing-social-media-shutdown/>).

Litigating the internet shutdown in Cameroon

In January 2020, the Internet was shut down in regions of Cameroon following protests against the arrest of civil society leaders resisting government efforts to impose the Francophone legal and education systems in predominantly Anglophone regions. The internet remained shut down for 93 days and was **switched** back on hours after Veritas Law filed a legal challenge with the Constitutional Council, with the assistance of Media Defence. The constitutional challenge was brought to compel the government to restore the Internet, and so that the Constitutional Council could prevent the government from shutting the Internet down in the future. Although the matter was eventually **dismissed** for lack of *locus standi*, it is an example of the potential positive impact of litigious efforts to hold the perpetrators of internet shutdowns to account, even where a positive judgment cannot be achieved.

In relation to the blocking and filtering of content, there may indeed be circumstances where such measures are justifiable, such as websites distributing child sexual assault material (**CSAM**). Such measures are still required to meet the three-part test for a justifiable limitation, which must be assessed on a case-by-case basis.⁴⁸

Similarly, limitations to network neutrality may also be permissible in certain circumstances, for example for legitimate network management purposes, or in circumstances in which zero rating is implemented fairly and transparently by public authorities with a mandate to do so and for a valid purpose. However, as a general principle, there should be no discrimination in the treatment of internet data and traffic, regardless of the device, content, author, origin and/or destination of the content, service, or application.⁴⁹ Further, internet intermediaries should be transparent about any traffic or information management practices they employ, and relevant information on such practices should be made available in a form that is accessible to all stakeholders.⁵⁰

It should also be noted that other, increasingly sophisticated ways to limit and control access to the internet and online content are also on the rise in Africa. This includes the adoption of social media taxes that increase prices for users and legal mandates for online publishers to register or obtain licenses, sometimes including all social media users.

NATIONAL SECURITY AS A GROUND OF JUSTIFICATION

National security is frequently relied upon as the justification for an interference with access to the internet, as well as other interferences with the right to freedom of expression.⁵¹ While

⁴⁸ For more on the three-part test, refer to Media Defence' Advanced Module 2 on Digital Rights and Freedom of Expression Online, which deals with restricting access and content.

⁴⁹ 2011 Joint Declaration above n 32 at para 5(a).

⁵⁰ *Id.* at para 5(b).

⁵¹ For a fuller discussion on national security more broadly see Richard Carver, 'Training Manual on International and Comparative Media and Freedom of Expression Law at p 77-88 (accessible here: <https://www.mediadefence.org/resources/mldi-manual-on-freedom-of-expression-law/>).

this may, in appropriate circumstances, be a legitimate aim, it also has the potential to be used to quell dissent and cover up state abuses.

The covert nature of many national security laws, policies, and decisions, as well as the refusal by states to disclose information about particular national security threats, tends to exacerbate this concern. Furthermore, courts and other institutions have often been deferent to the state in determining what constitutes national security. As has been previously noted:⁵²

“The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern. The concept is broadly defined and is thus vulnerable to manipulation by the State as a means of justifying actions that target vulnerable groups such as human rights defenders, journalists or activists. It also acts to warrant often unnecessary secrecy around investigations or law enforcement activities, undermining the principles of transparency and accountability.”

Principle 9(3) of the [Declaration of Principles on Freedom of Expression and Access to Information in Africa](#) provides that national security, public order, or public health are legitimate aims for a limitation on freedom of expression, but only if it is prescribed by law and necessary and proportionate. This means that it should:

- “(a) originate from a pressing and substantial need that is relevant and sufficient;
- (b) have a direct and immediate connection to the expression and disclosure of information, and be the least restrictive means of achieving the stated aim; and
- (c) be such that the benefit of protecting the stated interest outweighs the harm to the expression and disclosure of information, including with respect to the sanctions authorised.”

As set out in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (**Johannesburg Principles**), developed by a group of experts in international law, national security, and human rights, convened by ARTICLE 19, and endorsed by the then UNSR on freedom of expression:⁵³

- “(a) A restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to respond to the use or threat of force, whether from an external source, such as a military threat, or an internal source, such as incitement to violent overthrow of the government.
- (b) In particular, a restriction sought to be justified on the ground of national security is not legitimate if its genuine purpose or demonstrable effect is to protect interests unrelated to national security, including, for example, to protect a

⁵² Report of the UNSR on freedom of expression to the UNGA, A/HRC/23/40, 17 April 2013 at para 60 (accessible at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf).

⁵³ Principle 2 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information, November 1996 (accessible at <https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf>). The Johannesburg Principles were developed by a group of experts in international law, national security and human rights, convened by ARTICLE 19. It was endorsed by the then UNSR on freedom of expression.

government from embarrassment or exposure of wrongdoing, or to conceal information about the functioning of its public institutions, or to entrench a particular ideology, or to suppress industrial unrest.”

Principle 7 of the Johannesburg Principles goes further to state that the peaceful exercise of the right to freedom of expression shall not be considered a threat to national security or subjected to any restrictions or penalties.

Another important principle contained in the Johannesburg Principles is principle 23, which provides that: “[e]xpression shall not be subject to prior censorship in the interest of protecting national security, except in time of public emergency which threatens the life of the country”. As a general proposition, prior restraint of expression is impermissible. The measures described above can often give rise to a prior restraint on content, and consequently have a chilling effect on the enjoyment of the right to freedom of expression.

Similarly, counter-terrorism as a purported justification for network shutdowns or other interferences with access to the internet should also be treated with caution. As noted in General Comment No. 34, the media plays an important role in informing the public about acts of terrorism, and it should be able to perform its legitimate functions and duties without hindrance.⁵⁴ While governments may argue that internet shutdowns are necessary to ban the spread of news about terrorist attacks to prevent panic or copycat attacks, it has instead been found that maintaining connectivity may mitigate public safety concerns and help report public order.⁵⁵

At a minimum, if there is to be a limitation of access to the internet, there should be transparency regarding the laws, policies and practices relied upon, clear definitions of terms such as ‘national security’ and ‘terrorism’, and independent and impartial oversight being exercised.

INTERMEDIARY LIABILITY

Intermediary liability occurs when governments or private litigants can hold technological intermediaries, such as ISPs and websites, liable for unlawful or harmful content created by users of those services.⁵⁶ This can occur in various circumstances, including copyright infringements, digital piracy, trademark disputes, network management, spamming and phishing, “cybercrime”, defamation, hate speech, child pornography, “illegal content”, offensive but legal content, censorship, broadcasting and telecommunications laws and regulations, and privacy protection.⁵⁷

⁵⁴ General Comment No. 34 at para 46.

⁵⁵ 2017 Report of the UNSR on freedom of expression above n 18 at para 14.

⁵⁶ Alex Comninos, ‘The liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain’ (2012) at p 6 (accessible at: https://www.apc.org/sites/default/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL_0.pdf).

⁵⁷ *Id.*

A report published by UNESCO identifies the following challenges facing intermediaries:⁵⁸

- Limiting the liability of intermediaries for content published or transmitted by third parties is essential to the flourishing of internet services that facilitate expression.
- Laws, policies, and regulations requiring intermediaries to carry out content restriction, blocking, and filtering in many jurisdictions are not sufficiently compatible with international human rights standards for freedom of expression.
- Laws, policies, and practices related to government surveillance and data collection from intermediaries, when insufficiently compatible with human rights norms, impede intermediaries' ability to adequately protect users' privacy.
- Whereas due process generally requires that legal enforcement and decision-making are transparent and publicly accessible, governments are frequently opaque about requests to companies for content restriction, the handover of user data, and other surveillance requirements.

There is general agreement that insulating intermediaries from liability for content generated by others protects the right to freedom of expression online. Such insulation can be achieved either through a system of absolute immunity from liability, or a regime that only fixes intermediaries with liability following their refusal to obey an order from a court or other competent body to remove the impugned content.

As to the latter, the 2011 Joint Declaration provides that intermediaries should only be liable for third-party content when they specifically intervene in that content or refuse to obey an order adopted in accordance with due process guarantees by an independent, impartial, authoritative oversight body (such as a court) to remove it.⁵⁹ The [2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa](#) provides in Principle 39 that states should not require internet intermediaries to “proactively monitor content which they have not authored or otherwise modified” and to ensure that in moderating online content human rights safeguards are mainstreamed and all such decisions are transparently made with the possibilities for appeals and other remedies. It further provides that where law enforcement agencies request the immediate removal of online content because it poses an imminent risk of harm, such requests should be subject to judicial review.⁶⁰

While questions around intermediary liability have not yet been thoroughly considered by courts in Africa, a substantial body of jurisprudence is building up in other regions of the world, particularly Europe, Latin America, and India. For example, the ECtHR has considered intermediary liability in several cases:

- In 2013, in the case of [Delfi AS v Estonia](#), the ECtHR considered the liability of an internet news portal for offensive comments that were posted by readers below one of its online news articles.⁶¹ The portal complained that being held liable for the comments of its

⁵⁸ Rebecca MacKinnon et al, 'Fostering freedom online: The role of internet intermediaries' (2013) at pp 179-180 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000231162_eng).

⁵⁹ 2011 Joint Declaration above n 32 at paras 2(a)-(b).

⁶⁰ Principle 39.

⁶¹ Application No. 64569/09, 10 October 2013 (accessible at: <https://hudoc.echr.coe.int/eng/?i=001-155105>).

readers breached its right to freedom of expression. The ECtHR dismissed the case, holding that the finding of liability by the domestic courts was a justified and proportionate restriction of freedom of expression because the comments were highly offensive; the portal failed to prevent them from becoming public, profited from their existence, and allowed their authors to remain anonymous. It further noted that the fine imposed by the Estonian courts was not excessive.

- In 2016, in the case of *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, the ECtHR considered the liability of a self-regulatory body of internet content providers and an internet news portal for vulgar and offensive online comments posted on their websites.⁶² The ECtHR reiterated that, although not publishers of comments in the traditional sense, internet news portals still had to assume duties and responsibilities. The ECtHR found that, although offensive and vulgar, the comment had not constituted unlawful speech, and upheld the claim of a violation of the right to freedom of expression.
- In 2017, in the case of *Tamiz v United Kingdom*, the ECtHR had cause to consider the ambit of intermediary liability.⁶³ The applicant, a former politician in the United Kingdom, had claimed before the domestic courts that a number of third-party comments posted by anonymous users on Google's Blogger.com were defamatory. Before the ECtHR, the applicant argued that his right to respect for his private life had been violated because the domestic courts had refused to grant him a remedy against the intermediary. His claim was ultimately dismissed by the ECtHR on the basis that the resulting damage to his reputation would have been trivial. The ECtHR highlighted the important role that ISPs perform in facilitating access to information and debate on a wide range of political, social and cultural rights, and seemed to endorse the line of argument that ISPs should not be obliged to monitor content or proactively investigate potential defamatory activity on their sites.

⁶² Application No 22947/13, 2 February 2016 (accessible at: <https://hudoc.echr.coe.int/eng?i=001-160314>).

⁶³ *Tamiz v United Kingdom*, Application No. 3877/14, 19 September 2017 (accessible at: <https://hudoc.echr.coe.int/eng?i=001-178106>). Media Defence, together with a coalition of organisations, made submissions to the ECtHR on proposed principles for intermediary liability based on best practices in national legislation, the views of the Committee of Ministers of the Council of Europe (CoE) and special mandate holders.

The proposed principles are as follows:

- Intermediaries should not be the arbiters of the lawfulness of content posted, stored or transferred by the users of their services.
- Assuming that they have not contributed to or manipulated content, intermediaries should not be liable for content posted, stored or transferred using their services unless and until they have failed to comply with an order of a court or other competent body to remove or block specific content.
- Notwithstanding the above, intermediaries should in no circumstances be liable for content unless it has been brought to their attention in such a way that the intermediary can be deemed to have actual knowledge of the illegality of that content.
- A requirement to monitor content on an ongoing basis is incompatible with the right to freedom of expression contained in article 10 of the European Convention on Human Rights.

The submissions are accessible here:

<https://www.mediadefence.org/sites/default/files/blog/files/20160407%20Tamiz%20v%20UK%20Inter%20vention%20Filing.pdf>.

Other courts have taken more definitive positions in respect of intermediary liability. For example, the Supreme Court of India has interpreted the domestic law to only provide for intermediary liability where an intermediary has received actual knowledge from a court order, or where an intermediary has been notified by the government that one of the unlawful acts prescribed under the law are going to be committed and the intermediary has subsequently failed to remove or disable access to such information.⁶⁴ Furthermore, the Supreme Court of Argentina has held that search engines are under no duty to monitor the legality of third-party content to which they link, noting that only in exceptional cases involving “gross and manifest harm” could intermediaries be required to disable access.⁶⁵

The case of the non-consensual dissemination of intimate images (**NCII**), provides a challenge with regard to questions of intermediary liability. Courts around the world have frequently ordered the immediate and unequivocal removal of such content from online platforms, citing the significant and adverse consequences on victims’ and survivors’ rights to privacy and dignity. The High Court of Delhi, India, for example, ordered the immediate removal of content not only from the website on which it had been published, without consent, but also ordered search engines to de-index the content from their search results, stressing the need for “immediate and efficacious” remedies for victims of such cases.⁶⁶

This also relates to a concept known as ‘the right to be forgotten,’ which supporters argue creates an obligation on internet intermediaries to delete certain content on the request of a person who is the subject of such content. At present, the issue is being considered in multiple jurisdictions as the appropriate balance is sought between protecting the right to privacy and dignity and the right to access information of public importance.

In light of the vital role played by intermediaries in promoting and protecting the right to freedom of expression online, it is imperative that they are safeguarded against unwarranted interference — by state and private actors — that could have a deleterious effect on the right. For example, as an individual’s ability and freedom to exercise their right to freedom of expression online is dependent on the passive nature of online intermediaries, any legal regime that causes an intermediary to apply undue restraint or self-censorship toward content communicated through their services will ultimately have an adverse effect on the right to freedom of expression online. The UNSR has noted that intermediaries can serve as an important bulwark against government and private overreach, as they are usually, for instance, best-placed to push back on a shutdown.⁶⁷ However, this can only truly be realised in circumstances where intermediaries are able to do so without fear of sanction or penalties.

⁶⁴ *Shreya Singhal v Union of India*, Application No. 167/2012 at paras 112-118 (accessible at: <https://www.livelaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/>).

⁶⁵ *María Belén Rodríguez v Google*, Fallo R.522.XLIX (accessible at: http://www.stf.jus.br/repositorio/cms/portalStfInternacional/newsletterPortalInternacionalJurisprudencia/anexo/Fallo_R.522.XLIX_Corte_Suprema_da_Argentina_28_oct._2014.pdf). The decision has been described in the 2016 Report of the UNSR on Freedom of Expression at para 52.

⁶⁶ *X v. Union of India* (2021) (accessible at: <https://globalfreedomofexpression.columbia.edu/cases/x-v-union-of-india/>).

⁶⁷ 2017 Report of the UNSR on Freedom of Expression at para 50.

At the same time, it is vital that appropriate remedies are established for the removal of illegal or harmful content, and that powerful private platforms are held accountable for the decisions they make with regard to moderating content in the digital sphere, where such decisions may infringe on the rights to freedom of expression and access to information.

CONCLUSION

While the right of access to the internet does not yet find express recognition in international law, it is widely considered as an enabler of the right to freedom of expression and, as with all human rights, can only be justifiably limited if a three-part test is met. Additionally, restrictions to the internet may unduly infringe on freedom of expression and associated rights. In a rapidly developing digital world, the internet is increasingly becoming a contested space and is being leveraged equally by those seeking to defend fundamental rights and those seeking to limit them. An informed understating of concepts such as internet shutdowns, the blocking and filtering of content, net neutrality and intermediary liability are increasingly necessary to fully protect and promote the right to freedom of expression online.