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/

December 2020

TABLE OF CONTENTS

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 do not 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 where 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 whether the right of access to the internet are numerous.

Arguments in favour of access to the internet as a human right[1]	**Arguments against access to the internet as a human right**
• **Necessity**. There is a certain consensus on not only 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, eg. 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. These are most easily accessed online. • **Inseparability**. Technological progress changes how people enjoy their rights and governments should address the link between those rights and their current methods of enjoyment. • **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 to it. • **Public support**. Worldwide surveys show a single predominant attitude	• **No international treaty directly creates a right of access to the internet, although some countries, mostly in Europe, have domestic legislation that does**. 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 no discussion of a new treaty to do so in any forum. • **Analogy to other forms of media**. There is no right to the telephone, the television, the printed press (either for publishing or receiving it) or any other similar medium that has imposed a duty on states to provide it to its 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. • **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

[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/).

towards access to the internet: that it should be recognised as a right.[2]	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 with the ability to access the internet, therefore exacerbating inequalities. On the other hand, lack of control by governments would 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 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:[3]

[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).

[3] 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-

> "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".[4]

This has been expanded upon in the United Nation's 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".[5] 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,[6] and to strive to provide universal and affordable access to the internet in least developed countries by 2020.[7]

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 providing and expanding access to the internet.[8] Notably, it affirms the importance of applying a comprehensive rights-based approach in providing and in expanding access to the internet,[9] and calls on states to consider formulating and adopting national internet-related public

---

%20Recommendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf).

[4] 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).

[5] 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).

[6] *Id*. at goal 5(b) at p 18.

[7] *Id.* at goal 9(c) at p21.

[8] 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).

[9] *Id*. at para 5.

policies with the objective of universal access and the enjoyment of human rights at their core.[10]

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 firmly been 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 to be able to access the internet, inadequate locally-relevant content, insufficient levels of digital literacy, and a lack of political will to make this a priority.

In *Kalda v Estonia*, the European Court of Human Rights (ECtHR) held that the applicant's right to freedom of expression had been violated through a prison's refusal to grant him access to internet websites containing legal information, as this had breached his right to receive information.[11] The ECtHR noted that when a state is willing to allow prisoners access to the internet, as with the case in question, it had to give reasons for refusing access to specific sites.[12]

INTERFERENCES WITH ACCESS TO THE INTERNET

Some of the ways in which access to the internet is interfered with is 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, 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.[13] 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 effectively providing for the prohibition of most forms of prior restraint on speech.[14] The American Convention on Human Rights

[10] *Id.* at para 12.

[11] Application No. 17429, 19 January 2016 (accessible at: https://hudoc.echr.coe.int/eng?i=001-160270).

[12] *Id*. at para 53. In the subsequent decision of *Jankovskis v Lithuania*, Application No. 21575/08, 17 January 2017 (accessible at: https://hudoc.echr.coe.int/eng?i=001-170354), also in relation to a prisoner who had been refused access to a website containing education-related information, the ECtHR again upheld the applicant's claim of a violation of the right to freedom of expression.

[13] Council of Europe, 'Prior Restrains 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).

[14] 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 Preparatoires" of the International Covenant on Civil and Political Rights', Martinus Nijhoff (1987) at p 398.

contains a similar prohibition.[15] It is therefore imperative that, in order for any such measure 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.[16] 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.[17] 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 shutdown in its entirety. In other circumstances, this may also arise when access to mobile communications, websites or social media and messaging applications is blocked, throttled or rendered effectively unusable.[18] Shutdowns may affect an entire country, towns or regions within a country, or even multiple countries, and have been seen to range from several hours to several months.[19]

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.[20] 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 shutdown illegal

In a landmark case confirming that internet shutdowns constitute a form of prior restraint, in June 2020, the Economic Community of West African States (ECOWAS) Community Court of Justice ruled that the internet shutdowns implemented by the Togolese government in 2017 were illegal.[21]

---

[15] 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."

[16] Access Now, 'What is an internet shutdown?' (accessible at: https://www.accessnow.org/keepiton/?ignorelocale).

[17] *Id*.

[18] 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).

[19] *Id*.

[20] *Id*.

[21] 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).

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."[22]

For example, in March 2020 social media sites were blocked in Guinea during a referendum;[23] and in October that same year, a general shutdown of the internet ensued during the General Election.[24] 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.[25]

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.[26] In other words, ISPs should treat all data that travels over their networks fairly, without improper discrimination in favour of a particular application, website or service.[27] Discrimination in this regard may relate to affecting information in a way that halts, slows or otherwise tampers with the transfer of any data, except for a legitimate network management purpose, such as easing congestion or blocking spam.[28]

---

[22] 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).

[23] 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-keepiton-guinea-cuts-internet-access-and-blocks-social-media-on-referendum-day/).

[24] 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/).

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

[26] 2017 Report of the UNSR on freedom of expression above at n 18 at para 23.

[27] Electronic Frontier Foundation, 'Net neutrality' (accessible at: https://www.eff.org/issues/net-neutrality).

[28] American Civil Liberties Union, 'What is net neutrality?' (accessible at: https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality).

The 2017 Report of the UNSR on freedom of expression describes two key ways in which net neutrality may be affected:[29]

- **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; other services or applications, meanwhile, are subject to metered cost.

In various countries around Africa, there has been significant debate about access to zero-rated content, as particularly social networking sites 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 serve as a gateway to users to understand the opportunities that the internet can offer. On the other hand is that zero-rating can lead to unfair competition, and can distort users' perceptions by only allowing access to particular sites.[30]

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".[31] 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 that these limitations can cause:[32]

> "(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."

---

[29] 2017 Report of the UNSR on freedom of expression above n 18 at paras 24-28.

[30] 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).

[31] 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).

[32] International Mechanisms for Promoting Freedom of Expression, 'Joint declaration on freedom of expression and the internet', 1 June 2011 (2011 Joint Declaration).

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.[33] 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".[34]

As set out in General Comment No. 34:[35]

> "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 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 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.[36] 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.[37] In some countries, this has led to the government enacting new laws to expressly allow for shutdowns to take place.[38]

The UNSR on Freedom of Expression has further noted that network shutdowns invariably fail to meet the standard of necessity,[39] and are generally disproportionate.[40] States frequently seek to justify this on the ground of national security, which is discussed further below. For

---

[33] 2017 Report of the UNSR on freedom of expression above n 18 at para 8.

[34] 2016 UN Resolution on the Internet above n 8 at para 10.

[35] General Comment No. 34 at para 43.

[36] 2017 Report of the UNSR on Freedom of Expression at para 9.

[37] *Id.* at para 10.

[38] 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-Drn0MnxJAp58RoZoFI7u4L.html.)

[39] 2017 Report of the UNSR on freedom of expression above n 18 at para 14.

[40] *Id.* at para 15.

example, Chad blocked social media for a period of 472 days in 2018,[41] ostensibly for security reasons. A case was filed against two internet providers,[42] but access was restored shortly after.

Litigating the internet shutdown in Cameroon

Media Defence is currently assisting in litigating a case at the Constitutional Council of Cameroon. In January 2020, the Internet was shut down following protests against the arrest of civil society leaders resisting government efforts to impose the Francophone legal and education systems in these predominantly Anglophone regions. The Internet remained shut down for 93 days and was switched back on hours after Veritas Law filed the constitutional challenge. 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. You can read more here.

In relation to the blocking and filtering of content, there may indeed be circumstances where such measures are justifiable. For example, in relation to websites distributing child pornography. Such measures are still required to meet the three-part test for a justifiable limitation. This will need to be assessed on a case-by-case basis.

Similarly, limitations to network neutrality may also be permissible in certain circumstances, for example for legitimate network management purposes. 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.[43] 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.[44]

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.[45] While 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 practices, as well as the refusal by states to disclose information about the national security threat, tends to exacerbate this

[41] 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/).
[42] 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//).
[43] 2011 Joint Declaration above n 32 at para 5(a).
[44] *Id.* at para 5(b).
[45] 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/).

concern. Furthermore, courts and other institutions have often been deferent to the state in determining what constitutes national security. As has been previously noted:[46]

> "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 XIII(2) of the Declaration of Principles on Freedom of Expression in Africa provides that freedom of expression should not be restricted on public order or national security grounds "unless there is a real risk of harm to a legitimate interest and there is a close causal link between the risk of harm and the expression".

As set out in the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (the Johannesburg Principles):[47]

> "(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 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 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

---

[46] 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).

[47] 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.

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.[48] 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.[49]

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 where 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.[50] 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.[51]

A report published by UNESCO identifies the following challenges facing intermediaries:[52]

- 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

[48] General Comment No. 34 at para 46.

[49] 2017 Report of the UNSR on freedom of expression above n 18 at para 14.

[50] 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).

[51] *Id*.

[52] Rebecca MacKinnon et al, 'Fostering freedom online: The orle of internet intermediaries' (203) at pp 179-180 (accessible at: https://unesdoc.unesco.org/ark:/48223/pf0000231162_eng).

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.[53]

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.[54] The portal complained that being held liable for the comments of its 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.[55] 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.[56] The applicant, a former politician in the United Kingdom,

[53] 2011 Joint Declaration above n 32 at paras 2(a)-(b).

[54] Application No. 64569/09, 10 October 2013 (accessible at: httsp://hudoc.echr.coe.int/eng?i=001-155105).

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

[56] *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 based on best practices in national legislation, the views of the Committee of Ministers of the Council of Europe (CoE) and special mandate holders.

In the above case before the ECtHR, Media Defence together with a coalition of other organisations. 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.

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.

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.[57] 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.[58]

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,

---

- 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%20Intervention%20Filing.pdf.

[57] *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/).

[58] *María Belén Rodriguez 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.

best-placed to push back on a shutdown.[59] However, this can only truly be realised in circumstances where intermediaries are able to do so without fear of sanction or penalties.

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 it is used equally by those seeking to defend fundamental rights and those seeking to limit them. The proper 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.

[59] 2017 Report of the UNSR on Freedom of Expression at para 50.