Module 2

Restricting Access and Content

Advanced Modules on Digital Rights and Freedom of Expression Online

MEDIA DEFENCE

ISBN 978-0-9935214-1-6

Published by Media Legal Defence Initiative: www.mediadefence.org

This report was prepared with the assistance of ALT Advisory: https://altadvisory.africa/

Table of Contents

MODULE 2

Restricting Access and Content

- **To provide an overview of the current mechanisms through which access to the internet and access to content is restricted.**
- **To provide an overview of the fundamental international and regional legal principles.**
- **To understand the different rights implications of such restrictions.**
- **To set out the limitations of implicated rights and explore the justifiability of the measures adopted by states.**
- **To identify practical ways to deal with restrictions.**

Introduction

The internet was created to facilitate the free flow of information;[1] it now allows people to instantaneously access information and services, to communicate, and to share knowledge and ideas. The internet offers an array of opportunities for the realisation of human rights and has, in many instances, been a catalyst for the empowerment of marginalised members of society. It is common cause that the internet is an enabling space for the advancement of the right to freedom of expression, the right of access to information, the right of freedom of assembly, the right to freedom of opinion, thought and belief, the right to be free from discrimination in all forms, the right to education, the right to culture and language, and the right of access to socio-economic services. Access to the internet is of relevance in the African context and is a crucial component to social, economic and human development. The African Declaration on Internet Rights and Freedoms, a civil society initiative, calls for the internet to be accessible, available and affordable for all persons in Africa to benefit fully from its developmental potential.

However, there are growing impediments to this. Restrictions to access and internet disruptions are eroding the right to freedom of expression and associated rights.[2] Suppressive tactics by governments and private actors cause significant challenges in accessing information online. As will become apparent, the unjustifiable restriction of access to the internet is a violation of human rights. This module outlines some of the prevalent harms to access and provides guidance on how best to secure fundamental rights and freedoms in the digital age. In doing so, this module focuses on internet shutdowns, the ways in which access to content may be unjustifiably limited by employing blocking and filtering, the implications of social media taxes and the harms of distributed denial of service (**DDoS**) attacks.

---

[1] Internet Society, 'Brief History of the Internet' (1997) (accessible at: https://www.internetsociety.org/internet/history-internet/brief-history-internet/).
[2] See Tim Berners-Lee, 'I Invented the web. Here are three things we need to change to save it' (2017) (accessible at: https://www.theguardian.com/technology/2017/mar/11/tim-berners-lee-web-inventor-save-internet).

Internet Shutdowns

Overview of internet shutdowns

An internet shutdown typically involves the deliberate disruption of internet or electronic communications, to the extent they become inaccessible or unusable, generally targeting a particular population or within a specific location with the objective of exerting control over the free flow of information. Internet shutdowns, which are sometimes referred to as a "blackout" or "kill switch", include full and localised shutdowns, bandwidth throttling, and service-based blocking of two-way communication platforms.[3]

Internet shutdowns are on the rise—in 2019 reported incidents of internet shutdowns reached alarming numbers across the world highlighting the rise of this new trend in which governments seek to silence dissenting voices, control information and curb freedom of expression. Access Now reported 75 instances of internet shutdowns in 2016. This grew to 106 in 2017 and 196 in 2018. Access Now has further reported that in the first six months of 2019, there had already been 128 documented shutdowns. Of additional concern is the protracted duration of the shutdowns, with the shutdown in Kashmir in India lasting over 150 days, making it the most protracted recorded internet shutdown in a democracy.

Internet shutdowns are being used by states to limit opposition and disarm dissent and are often used during critical periods such as elections or protests. They pose severe threats to people's rights and are contrary to international human rights standards.

International and regional responses

Over the last decade, the use and prevalence of access to the internet has grown exponentially, and with this rise, there has been the corresponding development of international norms and standards regarding the use of the internet, and the various rights it invokes. In the context of internet shutdowns, the rights to freedom of expression, access to information, and association and assembly rights contained in articles 19 and 21 of the International Covenant on Civil and Political Rights (**ICCPR**) are primarily implicated.

In a 2011 Report, the United Nations Special Rapporteur on Freedom of Expression (**UNSR FreeEx**) reported to the United Nations General Assembly that—

> "the Internet has become a key means by which individuals can exercise their right to freedom of opinion and expression, as guaranteed by article 19 of the

[3] See Access Now, 'What is an internet shutdown?' (2019) (accessible at: https://www.accessnow.org/keepiton/?ignorelocale) and Media Defence, 'Training Manual on Digital Rights and Freedom of Expression Online'. See further Access Now, 'Launching STOP: the #KeepItOn internet shutdown tracker' (2017) (accessible at https://www.accessnow.org/keepiton-shutdown-tracker/) and Indian Council for Research on International Economic Relations, 'The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India' (2018) (accessible at https://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf).

> Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights."

In 2012, the UN Human Rights Council (**UNHRC**) unanimously adopted a Resolution to protect the free speech of individuals on the internet. This resolution was the first of its kind and notably called upon states to "promote and facilitate access to the Internet". It affirmed that—

> "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights".

In the last five years there have been more explicit statements concerning internet shutdowns:

- In 2016, the UNHRC expressed deep concern regarding "measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law."
- In 2017, the UNSR reported that: "Internet and telecommunications shutdowns involve measures to intentionally prevent or disrupt access to or dissemination of information online in violation of human rights law". The report explains further that shutdowns "ordered covertly or without an obvious legal basis violate the requirement of article 19(3) of the [ICCPR] that restrictions be 'provided by law'".
- In 2019, the UNHRC noted its deep concern with "the various forms of undue restriction of freedom of opinion and expression online, including where States have manipulated or suppressed online expression in violation of international law".
- In 2019, the UNSR reiterated that internet shutdowns are clearly inconsistent with article 19(3) of the ICCPR.

In an African context, the Special Rapporteur on Freedom of Expression and Access to Information in Africa has released an updated draft of the Declaration of Principles on Freedom of Expression in Africa which provides that:

> "States shall not interfere with the right of individuals to seek, receive and impart information through any means of communication and digital technologies, through measures such as removing, blocking and filtering of content, unless such interference is justifiable and compatible with international human rights law.
>
> States shall not engage in the wholesale disruption of access to the internet and other digital technologies for segments of the public or an entire population."

The above standards make it clear that internet shutdowns result in rights violations, and while these reports and resolutions are important for establishing the rights-based framework relating to internet shutdowns. The practicality of litigating against states requires a nuanced understanding of the international human rights standards of **legality**, **necessity**, and

proportionality and when there can be reasonable and justifiable limitations on fundamental human rights, particularly the right to freedom of expression. This is addressed below.

Legality, necessity and proportionality

Central to litigating internet shutdowns is establishing that it violates the right to freedom of expression and access to information, among others. As discussed above, internet shutdowns violate the full enjoyment of the right to freedom of expression. However, establishing this is not enough. The right to freedom of expression can only be limited when the limitation is provided by "law" and where "necessary" to ensure "respect of the rights or reputation of others" or for "the protection of national security or of public order (*ordre public*), or of public health or morals".

States often rely on "national security" or "public order" to justify internet shutdowns. When litigating the issue of internet shutdowns, it is important to conduct a thorough limitations analysis in order to illustrate to a court that a right has been infringed, and that the limitation does not meet the threshold of article 19(3) of the ICCPR.

Note on the limitation of freedom of expression

Article 19(3) of ICCPR sets out the grounds upon which the right to seek, receive and impart information and ideas on the internet may be limited. The restriction must be:

1. **Provided by law.**
2. **Be necessary for**:
   - Respect for the rights of others.
   - The protection of national security or of public order (*ordre public*), or of public health or morals.
     - ➔ These are understood as the "legitimate grounds for restrictions".

The UNHRC, through General Comment 34, has given further scope to the understanding of Article 19(3):

The restrictions must be provided by law:

- The law must be clear (be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly) and accessible, and apply equally to everyone.
- The law must also be consistent with international human rights law.
- It must provide sufficient guidance on remedies and procedures for challenging non-compliance with the law.
- It is for the state to demonstrate the legal basis for any restrictions imposed on freedom of expression.

The UNSR 2019 Report explains:

> "The restriction must be provided by laws that are precise, public and transparent; it must avoid providing authorities with unbounded discretion, and appropriate notice must be given to those whose speech is being regulated. Rules should be subject to public comment and regular legislative or administrative processes. Procedural safeguards, especially those guaranteed by independent courts or tribunals, should protect rights"

The restriction must be necessary:

- It must respect the rights or reputations of others. The UNHRC explains that for example, it may be legitimate to restrict freedom of expression in order to protect the right to vote. The UNHRC cautions that restrictions must be constructed with care: while it may be permissible to protect voters from forms of expression that constitute intimidation or coercion, such restrictions must not impede political debate, including, for example, calls for the boycotting of a non-compulsory vote.
- It must be aimed at the protection of national security or of public order (*ordre public*), or of public health or morals. Here the UNHRC explains that restrictive laws used for the pursuit of national security cannot be used to suppress or withhold from the public information of legitimate public interest if it does not harm national security. Journalists, researchers, environmental activists, human rights defenders, or others cannot be prosecuted for having disseminated such information if it does not harm national security.

The UNHRC explains further that the above grounds must conform to the strict tests of **necessity** and **proportionality:**

- Restrictions must be "necessary" for a legitimate purpose.
- Restrictions must not be overbroad. The UNHRC emphasised that restrictive measures must conform to the principle of proportionality:
    - They must be appropriate to achieve their protective function.
    - They must be the least intrusive instrument amongst those which might achieve their protective function.
    - They must be proportionate to the interest to be protected.
    - The principle of proportionality must be respected not only in the law that frames the restrictions but also by the administrative and judicial authorities in applying the law.

"Fundamentally, any restriction or limitation must not undermine or jeopardise the right to freedom of expression itself. Additionally, restrictions must be consistent with other rights found in the ICCPR and the fundamental principles found in the UDHR."[4]

[4] For more on this, including case discussions, see International Human Rights Program, 'Understanding the Right to Freedom of Expression: an internal law primer for journalists' (2014) at 30-5 (accessible at https://jhr.ca/wp-content/uploads/2019/10/Understanding-Freedom-of-Expression-Primer-ENG-web.pdf).

As indicated, any restrictions imposed on freedom of expression, including internet shutdowns, must be provided by law and must be necessary, clear and unambiguous and accessible. In this regard:

- Internet shutdowns may only be authorised by **law**. Directions or instructions from state departments or actors are insufficient to meet this legality threshold.
- The restriction must be **necessary**. Relying on the justification of national security to stifle advocacy and activism is prohibited and merely alleging the justification of national security is insufficient.
- The restrictions must also be **proportionate** to the purpose they seek to achieve. Internet shutdowns are seldom proportionate, and are generally viewed as a "disproportionate restriction on the right to freedom of expression, and have serious repercussions for the protection of other human rights."[5] For example, internet shutdowns disproportionately violate the rights of both a protester and a shop owner seeking to transact with mobile money. It is highly unlikely that a limitations analysis is equally applicable to these two people.

If a state cannot fulfil these requirements, then the restriction amounts to an unjustifiable and disproportionate limitation of the right. Echoing this and responding to the internet shutdown crisis in Kashmir, UN Special Rapporteurs have stated that "[t]he shutdown of the internet and telecommunication networks, without justification from the Government, are inconsistent with the fundamental norms of necessity and proportionality."

Recent examples of litigation relating to internet shutdowns

Despite these clear standards, states continue to claim that measures taken to restrict the internet are necessary and proportionate to ensure national security or public order, or both. Fortunately, there have been instances where courts have handed-down decisions providing that these justifications do not warrant internet shutdowns and where the threat of litigation itself has proved successful.

Cameroon

In 2017, a case was brought before the Constitutional Council in Cameroon which challenged the decision of the state to shut down the internet in the South West and North West of the country —the English speaking regions, following language-related protests. Civil society actors filed a challenge demanding that the state restore access to the internet in these regions, and keep it on. After the filing of the challenge, access to the internet was restored without the need for a judicial determination.

[5] ARTICLE 19 'The Right to Protest: Principles on the protection of human rights in protests' (2016) (accessible at https://www.article19.org/data/files/medialibrary/38581/Right_to_protest_principles_final.pdf) at 22.

Comments from the litigants

Media Defence along with Veritas Law were the applicants challenging the internet shut down. Media Defence stated:

> "The case that has been brought highlights that open and accessible internet communications are essential to ensuring the right to freedom of expression. Disruption of online services, whether through website blocking or internet shutdowns, amounts to a serious violation of that fundamental right. The government of Cameroon is obliged under domestic and international legal obligations to protect freedom of expression, including ensuring that it remains accessible and that people are able to use it freely and without interference."

In 2018, a renewed challenge was filed by Media Defence and Veritas Law which sought to emphasise that that state's actions in shutting down the internet was an infringement on the right to freedom of expression and a violation of international and regional human rights law.[6] The internet was ultimately restored, illustrating, as stated by Access Now "simply filing the lawsuit can get results, like increased transparency and responsiveness from telcos or the state."

Zimbabwe

In January 2019, an urgent chamber application was filed by Zimbabwe Lawyers for Human Rights (**ZLHR**) and the Media Institute of Southern Africa-Zimbabwe Chapter (**MISA-Zimbabwe**) challenging the ongoing internet shutdowns in Zimbabwe at that time. The Court granted an interim order that the implicated mobile operator must immediately and unconditionally resume full services and thus ensure access to the internet. The Court's ruling was mainly based on the absence of a legal provision enabling the shutdown.

Comments from the litigants

MISA-Zimbabwe stated:

> "It is now important that civil society, as MISA did, lobby parliament and the executive on digital rights, by pointing out how archaic Internet shutdowns are in trying to stop sharing information and that shutdowns do more harm to the country's reputation than good.
>
> It is imperative that free speech organisations have awareness campaigns, where they target influencers and community and thought leaders with a message that digital rights are as sacrosanct as the other rights in the

[6] CIPESA, 'Litigating Against Internet Shutdowns in Cameroon' (2018) (accessible at https://cipesa.org/2018/03/litigating-against-internet-shutdowns-in-cameroon/)

> constitution and the government should do all within its power to ensure that all freedoms are honoured."

Kashmir

The most recent and comprehensive case dealing with internet shutdowns is that of *Bhasin v Union of India; Azad v Union of India*. In 2019, internet services were disconnected in parts of Kashmir.

The petitioners approached the Supreme Court seeking, amongst other things:

- An order setting aside all orders, notifications, directions and / or circulars issued by the respondents under which any / all modes of communication including internet, mobile and fixed-line telecommunication services have been shut down or suspended or in any way made inaccessible or unavailable in any locality.
- An order directing the respondents to immediately restore all modes of communication including mobile, internet and landline services throughout Jammu and Kashmir in order to provide for an enabling environment for the media to practise its profession.

The questions of law that arose for the Supreme Court to consider were:

- Whether the government could claim an exemption from producing all orders pertaining to the suspension of telecommunications services.
- Whether freedom of expression and freedom to practise any profession or to carry on any occupation, trade or business over the internet constituted part of the fundamental rights under the Constitution.
- Whether the government's action of prohibiting internet access was lawful and valid.
- Whether the imposition of the relevant restrictions by the government were valid.
- Whether the freedom of the press of the petitioners was violated due to the restrictions.

In its ruling, the Supreme Court made some profound statements regarding freedom of expression and the intersection between law and technology:

> "Law and technology seldom mix like oil and water. There is a consistent criticism that the development of technology is not met by equivalent movement in the law. In this context, we need to note that the law should imbibe the technological development and accordingly mould its rules so as to cater to the needs of society.
>
> . . .
>
> We need to distinguish between the internet as a tool and the freedom of expression through the internet. There is no dispute that freedom of speech and expression includes the right to disseminate information to as wide a section of the population as is possible. The wider range of circulation of

> information or its greater impact cannot restrict the content of the right, nor can it justify its denial."

In addition, the Supreme Court conducted a thorough limitations analysis, noting that:

> "It goes without saying that the Government is entitled to restrict the freedom of speech and expression guaranteed under Article 19(1)(a) if the need be so, in compliance with the requirements under Article 19(2). It is in this context, while the nation is facing such adversity, an abrasive statement with imminent threat may be restricted, if the same impinges upon the sovereignty and integrity of India. The question is one of extent rather than the existence of the power to restrict."

The Supreme Court found that freedom of speech and expression and the freedom to practice any profession or carry on any trade, business or occupation over the medium of the internet enjoys constitutional protection and any restriction upon such fundamental rights should be in consonance with the restrictions provided for in the Constitution, inclusive of the test of proportionality.

Ultimately, a list of directions was issued by the Supreme Court, including a declaration that suspending internet services indefinitely is impermissible, and can be for a temporary duration only; suspending the internet in terms of the "Suspension Rules" must adhere to the principle of proportionality and must not extend beyond the necessary duration; any order suspending or restricting access to the internet is subject to judicial review; and the state was directed to review all orders suspending internet services.

Commentary – did the judgment go far enough?

The Software Freedom Law Centre, India (SFLC.In) welcomed the judgment but noted some concerns:

1. The direction to review the suspension orders could be a futile exercise as the review committee is composed of members exclusively from the executive.
2. The judgment did not give any immediate relief to the people in Kashmir.

Former Chief Justice, Justice Shah of the Delhi High Court stated, during the Fourth LC Jain Memorial Lecture, that the judgment is laudable in many respects, but went on further to state:

> "Unfortunately, despite these observations, the Supreme Court failed to actually decide the matter. The purported reason seems to be that it did not have all the orders in front of it, and the situation was changing on the ground daily. However, this reasoning seems tenuous, when we consider that a few sample shut down orders were placed before it (with detailed arguments being made about their unconstitutionality), and the Court could have easily directed the government to file the remaining orders.

While the reliance on Lon Fuller's famous statement that "there can be no greater legal monstrosity than a secret statute" is praiseworthy, it did not result in any practical benefit, given that the government was effectively allowed to take advantage of its own wrong of not publishing all the orders or submitting it before the Supreme Court.

After ruling that the suspension of communication services must adhere to the principles of necessity and proportionality, the Court failed to apply these principles to actually decide the legality of the communication shutdown in Kashmir.

Instead, it directed the fresh publication of all orders, with the Review Committee reviewing all these orders. The reliance on Lord Diplock's aphorism "you must not use a steam hammer to crack a nut, if a nutcracker would do", was, at least for the people of Kashmir, meaningless."

Overall, this judgment has been widely welcomed. It provides a comprehensive discussion on the topic of internet shutdowns, and it is useful to future litigants who are faced with these issues. It evinces that change can be effected through litigation.

In conjunction with litigation considerations, there are some other practical tips which may be of use, particularly in relation to capturing and preserving video evidence during internet shutdowns. These tips can be useful for establishing a rights violation and pursuing litigation.

Tips to consider when litigating this issue

The Southern African Litigation Centre recently prepared a report on navigating litigation during internet shutdowns in Southern Africa which highlights the legal considerations relevant for challenging internet shutdowns in courts in the region.

- **The parties**: consider the impact of the shutdown and if it is necessary to identify specific categories of applicants and respondents. Identify who is responsible for ordering the shutdown and who implemented it.
- **The procedure and the relief**: consider if the case requires urgent litigation and interdicts, injunctions or judicial reviews. Consider the type of precedent the case will set.
- **The law**: consider whether there are existing laws that prescribe for blockage orders. If there are, consider whether the government has complied with them and consider if the laws themselves are in accordance with human rights standards.
- **The rights**: consider which rights were violated and consider responses to government justifications.

Tips for documenting internet shutdowns

Witness has released a blog series with practical tips for documenting internet shutdowns:

- **Prepare your device**: learn about setting your phone up for offline documentation. This can include learning how to encrypt your device, ensuring that your phone has appropriate security settings and installing apps when there is no internet.
- **Understand what happens to the content that you capture**: learn about identifying which apps can and should be used to in the event of an internet shutdown. It is helpful to know who the app developer is, where your data will be stored, and whether meta-data is captured when there is no access to the internet. Learn about backing up your phone's media without the internet or a computer; this is an important safeguard against accidental deletion, corrupted data or if a device is confiscated.
- **Maintain verifiable media during an internet shutdown**: learn about ways to ensure that your documentation can be verified and corroborated given that you might only be able to upload it at a later stage. This can include capturing identifying details (landmarks, street signs, newspapers that illustrate the date), including a description of the meta-data and keeping backups.
- **Share and communicate content:** learn about some methods and approaches for offline sharing and communication. This can include sharing files via Bluetooth Wifi Direct, or Near Field Communication, using a wireless hard drive or flash drive and using peer-to-peer messaging apps.

Conclusion

The growing number of shutdowns internationally and in Africa is of grave concern. Fortunately, there is a simultaneous growth of activism and litigation that is working towards curbing these continued rights violations. Until states refrain from blanket bans in access to the internet through shutdowns, strategic litigation and activism should persist and continue to grow and should be coupled with appropriate advocacy strategies.

Access to Content: Censorship, Blocking and Filtering

Overview of censoring, blocking and filtering of content

Access to information, and increasingly access to knowledge, is a central tenet of the internet. However, efforts to restrict access have developed in step with increased access. Technical measures are being implemented by state and non-state actors to limit, influence, monitor and control people's access to the internet. These measures include censoring, blocking, filtering and monitoring content. While these measures may not be as extreme as complete internet shutdowns, they equally hinder the full enjoyment of the right to freedom of expression.

Censorship and blocking	Filtering
Typically refers to the prevention of access to specific websites, domains, IP addresses, protocols or services included on a blacklist.[7] Justifications for blocking often include the need to prevent access to illegal content, or content that is a threat to public order or is objectionable for a particular audience.[8]	Generally refers to restricting or limiting access to information (or related services) that is either illegal in a particular jurisdiction, is considered a threat to public order, or is objectionable for a particular audience. Filtering can relate to the use of technology that blocks pages by reference to certain characteristics, such as traffic patterns, protocols or keywords, or based on their perceived connection to content deemed inappropriate or unlawful.
Note: This distinction might be considered semantical, but it can also be considered a matter of scale and perspective. However, the key commonality is that they both limit access to the internet.[9]	

As explained by ARTICLE 19, there are different ways in which access to content can be restricted, for example:[10]

- URL blocking blocks a specific web page.
- IP address blocking prevents connection to a host.
- Entire domain names can be blocked through DNS tampering.
- Blacklisting compiles a list of URLs to be filtered, while whitelisted URLs are not subject to blocking or filtering.
- Keyword blocking is generally used to enable the blocking of specific categories of content.

The rise of disinformation has also contributed to an increase in blocking and filtering with states trying to mitigate the spread of false information, and in some instances legally permitting blocking and filtering in order to prohibit and punish the dissemination of false or inaccurate statements.

Applicable international human rights standards

The same general considerations relating to access, online rights and freedom of expression discussed above are applicable here, save for specific considerations relating to filtering and

[7] ARTICLE 19, 'Freedom of Expression Unfiltered: How blocking and filtering affect free speech' (2016) at 7 (accessible at https://www.article19.org/data/files/medialibrary/38586/Blocking_and_filtering_final.pdf).
[8] Internet Society, 'Internet Society Perspectives on Internet Content Blocking: An Overview' (2017) (accessible at https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/).
[9] Id. See further Barnes, 'Technical Considerations for Internet Service Blocking and Filtering' (2013) (accessible at https://tools.ietf.org/id/draft-iab-filtering-considerations-03.html).
[10] ARTICLE 19 above n 7 at 9.

blocking. In 2011, in a Joint Statement on Freedom of Expression and the Internet, a collective of Special Rapporteurs and experts stated the following in relation to filtering and blocking:

- Mandatory blocking of entire websites, IP addresses, ports, network protocols or types of uses (such as social networking) is an extreme measure – analogous to banning a newspaper or broadcaster – can only be justified in accordance with international standards, for example, where necessary to protect children against sexual abuse.
- 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.
- Products designed to facilitate end-user filtering should be accompanied by clear information to end-users about how they work and their potential pitfalls in terms of over-inclusive filtering.

In a 2016 Report, the UNSR on FreeEx explained that:

> "States often block and filter content with the assistance of the private sector. Internet service providers may block access to specific keywords, web pages or entire websites. On platforms that host content, the type of filtering technique depends on the nature of the platform and the content in question. Domain name registrars may refuse to register those that match a government blacklist; social media companies may remove postings or suspend accounts; search engines may take down search results that link to illegal content. The method of restriction required by Governments or employed by companies can raise both necessity and proportionality concerns, depending on the validity of the rationale cited for the removal and the risk of removal of legal or protected expression.
>
> Ambiguities in State regulation coupled with onerous intermediary liability obligations could result in excessive filtering. Even if content regulations were validly enacted and enforced, users may still experience unnecessary access restrictions. For example, content filtering in one jurisdiction may affect the digital expression of users in other jurisdictions. While companies may configure filters to apply only to a particular jurisdiction or region, there have been instances where they were nevertheless passed on to other networks or areas of the platform."

Blocking and filtering in Ethiopia

Ethiopia has been regarded as a problematic state in relation to its use of blocking and filtering in the past. Between 2012 and 2018, hundreds of websites were blocked, including the websites of LGBTIQ organisations, media outlets and CSOs like the Electronic Frontier Foundation. In 2017, during a spate of anti-government protests, Facebook, Twitter, WhatsApp, and Dropbox were frequently blocked.

In 2018 Freedom House noted that with the change of regime, over 250 websites were unblocked. Despite this, politically motivated blocking and filtering remains a threat in Ethiopia. As of 2019, Freedom House confirmed that there were still no procedures for determining which websites are blocked or for appealing blocking decisions.

Blocking and filtering in Turkey

Turkey's government has recently received sustained criticism for the "systematic actions the Turkish government has taken to restrict Turkey's media environment, including closing media outlets, jailing media professionals, and blocking critical online content."[11] In 2018, Freedom House found that over 3300 URLs containing news items were blocked.

In 2019, the Wikimedia Foundation, which owns and operates Wikipedia, petitioned the European Court of Human Rights (**ECtHR**) in relation to the blocking of Wikipedia in Turkey. Despite the outstanding petition to the ECtHR, in January 2020, following a ruling from the Turkish Constitutional Court, the Turkish government restored access to Wikipedia. The Constitutional Court ultimately found that blocking Wikipedia was unconstitutional.

Concerns of blocking and filtering in 2020 Togolese Elections

Presidential elections were held in Togo in February 2020. There were heightened tensions in the lead up to the elections, with protests against the 53-year rule of Gnassingbe Eyadema. In a joint letter to the government of Togo, CSOs noted their concerns that the Togolese government would restrict access to the internet during the elections. Reports suggest that it is highly likely that social media platforms such as WhatsApp, Telegram, and Facebook messenger were blocked on the day of elections.

Blocking and filtering remain a contemporary concern. While in limited instances there may be justifiable limitations, the trend is that of generally unjustifiably blocking and filtering with limited guidance to the public and limited to no regulation or oversight over the state.[12]

[11] U.S. Mission to the United Nations 'Remarks at a UN Third Committee Dialogue with the Special Rapporteur on the Freedom of Expression' (2019) (accessible at https://usun.usmission.gov/remarks-at-a-un-third-committee-dialogue-with-the-special-rapporteur-on-the-freedom-of-expression/)

[12] UNICEF 'Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information and Participation (2017) at 11 (accessible at https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_EXPRESSION.pdf).

Unjustifiable limitations

There may be circumstances where measures such as blocking and filtering of content are justifiable. The protection of children's rights may be one such justification. Blocking and filtering techniques can be developed and utilised to prevent the proliferation of and exposure to damaging material and to protect children from harmful and illegal content. However, despite this important purpose, UNICEF's 2017 Report on 'Children's Rights and Business in a Digital World: Freedom of Expression, Association, Access to Information and Participation' has recognised the inherent concerns around blocking and filtering, including a lack of transparency; the unscrupulous nature of filters; the lack of evidence to show where and when they have been deployed; and the threat of legitimate content being limited.[13] The children's rights example illustrates that even when there might appear to be a legitimate purpose, rights can be unduly limited if the elements of legality, necessity and proportionality are not thoroughly and independently tested.

As discussed above, and as with all limitations of the right to freedom of expression, restrictions are only permissible if they are provided by **law**, pursuant to a legitimate aim and conform to the strict tests of **necessity** and **proportionality**. In terms of "blanket" or "generic" bans, the 2011 UNHRC General Comment found that "generic bans on the operation of certain sites and systems are not compatible" with article 19 of the ICCPR. Where restrictions constitute "generic" bans, they will generally amount to an infringement of the right to freedom of expression.

In digital rights litigation, practitioners will do well to test all tenets of the limitations analysis before determining the appropriateness or otherwise of an imposed restriction. The ECtHR, in its 2012 decision of *Ahmet Yıldırım v Turkey*, provides guidance on the limitations analysis in relation to blocking and filtering.

Case note: *Ahmet Yıldırım v Turkey*

The applicant owned and ran a website on which he published his academic work and his views on various topics. In 2009, the Denzili Criminal Court in Turkey ordered the blocking of the website as a preventative measure in the context of criminal proceedings against the site's owner, who was accused of insulting the memory of Atatürk. The Court subsequently ordered the blocking of all access to *Google Sites*, a website hosting platform, as this was the only means of blocking the offending website. The applicant unsuccessfully tried to have the blocking order removed and applied to the ECtHR submitting that the blocking of *Google Sites* amounted to indirect censorship.

The ECtHR held that the impugned measure amounted to a restriction stemming from a preventive order blocking access to a website. The ECtHR found that the impugned measure produced arbitrary effects and could not be said to have been aimed solely at blocking access to the offending website, since it consisted in the wholesale blocking of all websites hosted by *Google Sites*.

[13] Id at 12.

The ECtHR reasoned that specific legal provisions are necessary, as general provisions and clauses governing civil and criminal responsibility do not constitute a valid basis for ordering internet blocking. Relying on General Comment 34, the Joint Declaration on Freedom of Expression and the Internet and the 2011 UNSR FreeEx Report, the ECtHR went further, stating:

> "In any case, blocking access to the Internet, or parts of the Internet, for whole populations or segments of the public can never be justified, including in the interests of justice, public order or national security. Thus, any indiscriminate blocking measure which interferes with lawful content, sites or platforms as a collateral effect of a measure aimed at illegal content or an illegal site or platform fails *per se* the "adequacy" test, in so far as it lacks a "rational connection", that is, a plausible instrumental relationship between the interference and the social need pursued. By the same token, blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship."

Furthermore, the ECtHR held that the judicial review procedures concerning the blocking of websites in Turkey are insufficient to meet the criteria for avoiding abuse, as Turkish domestic law does not provide for any safeguards to ensure that a blocking order in respect of a specific website is not used as a means of blocking access in general. Accordingly, the ECtHR found there had been a violation of the right to freedom of expression.

Similar considerations relating to ligation in respect of internet shutdowns are applicable in the context of blocking and filtering. However, there are further practical considerations that might be of use to potential litigators and activists.

Tips for measuring restrictions

The Open Observatory of Network Interference is a useful, free resource that detects censorship and traffic manipulation on the internet. Their software can help measure:

- Blocking of websites.
- Blocking of instant messaging apps (WhatsApp, Facebook Messenger and Telegram).
- Blocking of censorship circumvention tools (such as Tor).
- Presence of systems (middleboxes) in your network that might be responsible for censorship and/or surveillance.
- Speed and performance of your network.

This tool can be a helpful way to collect data that can be used as evidence of restrictions to access.

Conclusion

Activists and litigators should remain vigilant in relation to blocking and filtering and, where necessary, apply the principles of legality, proportionality and necessity to establish when the restriction of content amounts to a rights violation. As international pressure against internet shutdowns mounts, litigators should be cognisant that blocking and filtering may increase as an attempt to restrict the free flow of information.

Social Media Taxes

Overview of social media taxes

Social media taxes, as the name indicates, is a recently conceived tax on social media users. This has been a growing trend in Africa, with Uganda leading the way with the introduction of the Excise Duty (Amendment) Act 2018. This Act envisages that "a telecommunication service operator providing data used for accessing over the top services is liable to account and pay excise duty on the access to over the top services." Taxing over-the-top services (**OTTs**) is supposedly set to create a level playing field among telecommunications service providers and to favour local content over international content.

While there is still uncertainty around the practicalities of the tax, what is apparent is that it will "disproportionately and negatively impact the ability of users in Uganda to gain affordable access to the internet, and thus unduly restrict their right to freedom of expression."[14] Kenya and Tanzania appear to be following suit with the imposition of social media taxes and other regulations, which may restrict access.

This trend has sparked concern among digital rights activists and individual users alike. There are clear rights-based implications for the use of social media. The additional financial burden will curb people's access and enjoyment of online content, and it may also diminish their ability to access information and exchange ideas. Human Rights Watch has expressed concern that the proposed tax is "just another way for authorities to stifle free speech", explaining that "[t]axing anyone to use social media is an affront to their basic human rights. Uganda can try to dress up this draconian new tax as a benefit, but, in reality, it is just another clumsy attempt to limit free speech."[15]

Human rights implications of social media taxes

The international human rights framework on access to the internet and the promotion of the right to freedom of expression has been discussed, in detail, above. The same principles apply here, save for the addition of a brief review of the African human rights system.

[14] ARTICLE 19 'Eastern Africa new tax and licensing rules for social media threaten freedom of expression' (2018) (accessible at https://www.article19.org/resources/eastern-africa-new-tax-and-licensing-rules-for-social-media-threaten-freedom-of-expression/).
[15] Human Rights Watch 'Uganda's Troubling Social Media Tax
New Law Restricts Right to Free Speech and Information on Social Media' (2018) (accessible at https://www.hrw.org/news/2018/07/02/ugandas-troubling-social-media-tax).

In 2016, the African Commission on Human and Peoples' Rights (**ACHPR**) adopted a Resolution on the Right of Freedom of Information and Expression on the Internet in Africa. The Resolution recalls the 2012 United Nations Human Rights Council Resolution, discussed above, and affirms that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice." The Resolution recognises the importance of the internet in advancing human and peoples' rights in Africa, particularly the right to freedom of information and expression.

In 2018, the ACHPR expressed concern regarding the growing trend of states in East Africa adopting stringent regulations on the internet and internet platforms. The ACHPR noted particular concern over the following developments:

- The Electronic and Postal Communications (Online Content) Regulations 2018 in Tanzania, which introduced licensing requirements for bloggers who are now required to pay up to 2,100,000 Tanzanian Shillings (around USD900) for licences.
- The Excise Duty (Amendment) Bill 2018 in Uganda, which requires users of OTTs, such as social media platforms, to pay UGX200 (USD0.05), per user, per day of access.
- The directive issued by the Kenya Film and Classification Board on 14 May 2018 requiring licences for anyone posting videos for public exhibition or distribution online on their social media accounts.

The ACHPR further stated:

> "These regulations may negatively impact the ability of users to gain affordable access to the Internet, which goes against States' commitment to protect the right of every individual to receive information, as well as the right to express and disseminate one's opinion within the law which is provided under Article 9 of the African Charter on Human and Peoples' Rights."

In 2019, the Special Rapporteur on Freedom of Expression and Access to Information in Africa issued a press release on the continuing trend of internet and social media shutdowns in Africa. While this press release was directed more at internet shutdowns, it provided a useful reminder that "the internet and social media have given voice to the people of Africa who may now discourse on social, economic and political issues far more than ever before, and states should not take away that voice."

Recent examples in Africa

Uganda

As briefly discussed above, Ugandans are required to pay 200 shillings a day (about 0.05 USD) to access OTT services, which include social networking and messaging apps.[16] In

[16] CIMA, 'How Social Media Taxes Can Burden News Outlets: The Case of Uganda' (2019) (accessible at https://www.cima.ned.org/publication/how-social-media-taxes-can-burden-news-outlets-the-case-of-uganda/).

January 2020, the Uganda Revenue Authority reportedly proposed that the OTTs tax be transformed into a fully-fledged tax on internet data to be paid by users.

Of the approximately 45 million people in Uganda, nearly 25 million have a mobile subscription and around 19 million are internet users. Given that Uganda is a developing country, it is difficult to understand why the state has resolved to tax individual users rather than profitable foreign-based social media platforms or even local digital media publishers. The tax is significant and diminishes access to, and affordability of, the internet for the majority of Uganda's population.[17] The implications for the right to freedom of expression are clear.[18]

Estimated impact of the tax

It appears that the Ugandan Tax Authority reported that within a year of the tax being introduced, it has only received 17% of the anticipated revenue. Reportedly, it appears that many social media users are relying on virtual private networks (**VPNs**) to avoid the financial implications of the tax.

Kenya

The Kenyan Film and Classification Board requires citizens to obtain a license to be able to post videos on the internet. The Board has explained that it seeks to protect national security from illegal filming activities, as well as provide an additional stream of revenue. The additional cost raises concerns about the ability of video producers to operate, including concerns that this could have far-reaching consequences for freedom of expression online.

Potential developments to monitor in Kenya

The Kenya Information and Communication (Amendment) Bill 2019 is presently before Parliament. The Bill seeks to introduce regulations relating to the licensing of social media platforms and sharing of information by licensed persons. The Bill aims to create obligations on social media users, requires the registration of bloggers, and allows the Communications Authority to develop a bloggers code of conduct. The Board appears to be calling for the adoption of this legislation. The Board's CEO has indicated that "social media is a threat to the country's moral fabric as it negatively influences the youth."

[17] APC, 'Human rights impacts of taxing popular internet service' (accessible at https://www.apc.org/sites/default/files/Human_rights_impacts_of_taxing_popular_internet_services_0.pdf).
[18] ARTICLE 19 update (2020) (accessible at https://www.article19.org/resources/ugandas-proposed-tax-on-internet-data-threatens-the-rights-to-freedom-of-expression-and-access-to-information/). See Uganda Business News, 'Week in review: Trade disputes, social media tax, African internet registry' (2020) (accessible at https://ugbusiness.com/7993/week-in-review-trade-disputes-social-media-tax-african-internet-registry).

Tanzania

Tanzania has also introduced licensing requirements which attach additional fees to social media. The Electronic and Postal Communications (Online Content) Regulations introduced new online content regulations. Bloggers, in particular, are required to pay unreasonably high fees in order to obtain a license. Among other concerns with the regulations, the licensing requirement has been heavily criticised for being incompatible with the right to freedom of expression. The Association for Progressive Communications (**APC**) argues that:

> "Tanzania's new excise duty in the form of online content licence fees fundamentally threatens universal access to and affordability of the internet. Consequently, it clearly constitutes a limitation on the right to freedom of expression. Further, it is unjustifiable when measured against the arguments that could be made by the Tanzanian government in support of the increase, such as the need to ensure appropriate excise duty levels in order to ensure the fiscal sustainability of the state in meeting the developmental and other socioeconomic rights of its inhabitants."[19]

Attempts to oppose the Regulations

- In 2018, ARTICLE 19 reviewed the Tanzania Regulations. The report ultimately found that they were defective and wholly at odds with international standards on freedom of expression. ARTICLE 19 recommended that the Regulations should be withdrawn entirely and called on the Tanzanian government to do so.
- In April 2018, Reuters reported that civil society activists obtained a temporary court injunction against the regulations from Tanzania's High Court that would require bloggers to, among other things, pay a tax, obtain a clearance certificate and obtain an operating license.
- In May 2018, Reuters reported that the Tanzanian government overturned the injunction. As a result, owners of social media platforms are required to register and comply with the regulations.

Conclusion

The trend of introducing social media taxes in Africa warrants concern. There appears to be a misnomer that states can wilfully ignore their obligation to respect, protect and promote the right to freedom of expression in pursuit of economic gain. The ACHPR, civil society actors and affected individuals should continue to speak out against these trends. Litigation, policy reform and advocacy strategies need to be urgently adopted to re-route the current trajectory away from increased reliance by states on social media taxes.

[19] APC above n 17 at 12.

Distributed Denial-of-Service Attacks

Overview of DDoS attacks

The UNSR on FreeEx defines a DDoS attack as a cyber-attack that seeks to undermine or compromise the functioning of a computer-based system.[20] The UNSR notes further that a DDoS attack can have the same effect as an internet shutdown. This increasingly common online phenomenon uses a large number of computers to target websites and online services and overwhelms them with more traffic than they can handle rendering them temporarily inoperable.[21]

DDoS Attacks and critical moments

The 2019 UNSR Research Paper on Freedom of Expression and Elections in the Digital Age found:

> "During elections, State actors have historically denied access to unfavourable views and information concerning incumbent officeholders. In the digital age, technological advances have enabled perpetrators to increase the scope and frequency of these attacks on freedom of expression. One common practice involves the use of Distributed Denial of Service ("DDoS") attacks, where a network of online systems is compromised and directed to flood another online system with Internet traffic, effectively rendering the target inaccessible. These attacks have targeted the websites of political parties, journalists and media outlets, and human rights defenders and civil society organizations. Perpetrators have also targeted the websites of States' election commissions, which publicize critical information such as changes to ballot locations. DDoS attacks are also potentially a cover for coordinate hacks on voter registration and other electoral databases and other attempts to steal the data of voters, candidates and public officials. Given that online media have become the primary resource of news and information for many voters, and the integration of electronic systems into electoral processes, DDoS attacks are likely to increase in magnitude and frequency. Furthermore, in the Internet of Things era, the growing number of connected devices makes them attractive targets for DDoS attacks."

Given their similarity to internet shutdowns, DDoS attacks, whether committed by a state or non-state actor, infringe the right to freedom of expression. They are usually well hidden, covert and illicit in nature, and, accordingly, fall foul of the "provided by law" requirement of article 19(3) of the ICCPR. They completely disable access to online content, usually during a critical time – such as an election – and they are distinctly disproportionate. The UNSR Research Paper further found that DDoS attacks "whether committed by State actors or their

[20] Access Now, 'Defending users at risk from DDoS attacks: An evolving challenge' (2015) (accessible at https://www.accessnow.org/defending-users-at-risk-from-ddos-attacks-an-evolving-challenge/).
[21] See further Media Defence above n 3 at 23.

agents, are incompatible with Article 19 of the ICCPR" and are "almost always unnecessary and disproportionate measures under Article 19(3)."

The Inter-American Commission on Human Rights reported in 2013 that DDoS attacks can be extremely disruptive to the exercise of the right to freedom of expression, and, as a result, states are obligated to investigate and properly redress such attacks. The principles mentioned above and sentiments relating to access and freedom of expression are implicated by DDoS attacks. The UN Guiding Principles on Business and Human Rights can also be relied on when trying to prevent and mitigate DDoS attacks by non-state actors, including the safeguarding of systems infrastructure.

Recent DDoS attacks

In 2017, Freedom House reported:

> "Independent blogs and news websites are increasingly being taken down through distributed denial-of-service (DDoS) attacks, activists' social media accounts are being disabled or hijacked, and opposition politicians and human rights defenders are being subjected to surveillance through the illegal hacking of their phones and computers. In many cases, such as in Bahrain, Azerbaijan, Mexico, and China, independent forensic analysts have concluded that the government was behind these attacks."

DDoS attacks are affecting states across the world, regardless of their social policies or economic status. In 2018, it was reported that a website of a Mexican political opposition party was rendered inoperable by a DDoS attack. The attack occurred during a debate between presidential candidates in the lead up to the elections. In 2019, the South African financial sector fell victim to a string of DDoS attacks. Additionally, DDoS attacks were ranked among the top five security threats in Kenya in 2019. British political parties were also subject to back-to-back DDoS attacks in the lead up to the general election in 2019.

Conclusion

Be it politically, socially or economically motivated, DDoS attacks are a legitimate threat to freedom of expression. Nefarious state and non-state actors are becoming increasingly skilled and sophisticated, posing new challenges for states to overcome in order ensure they fulfil their positive obligations to protect and promote freedom of expression. Mitigating DDoS attacks in future will take multidisciplinary teams of litigators and technologists working jointly to protect and promote freedom of expression.

Conclusion

The internet is a site of struggle for the advancement of human rights. Restricting access to the internet, either through internet shutdowns, blocking and filtering or imposing regulatory restrictions or facilitating DDoS attacks limits people's fundamental human rights. The promotion, protection and enjoyment of human rights on the internet is well established, and

restricting of access to the internet, by states or non-state actors, violates human rights and can only be justified under very narrow circumstances.

It is comforting to observe that despite the rise of restrictive conduct, the international community, civil society actors and individuals are fighting to advance freedom of expression and digital rights. Fortunately, there are strong legal foundations that allow for progressive and dynamic solutions to these contemporary challenges.