4

Internet shutdowns and digital citizenship

Felicia Anthonio and Tony Roberts

Introduction

An internet shutdown is an intentional disruption of connectivity that prevents the free flow of information and communication. Ordered by governments and implemented by mobile and internet companies, internet shutdowns are a violation of fundamental human rights, including the freedom of expression, communication and association. As social, economic and political life is increasingly conducted online, the costs of connectivity disruption to businesses, families and democracies can be devastating, yet the use of internet shutdowns is becoming more frequent; they are lasting longer and are evolving to take on new forms. Access Now and the #KeepItOn coalition have documented at least 935 incidents of shutdowns in 60 countries globally from January 2016 to December 2021 (Guest 2022). Around 34 African countries accounted for 120 incidents of the shutdowns recorded during this period. This will be discussed in detail in the next section.

The chapter begins with a review of concepts of citizenship and digital citizenship and explores what particular action possibilities or 'affordances' digital technologies provide for citizenship. Having established this conceptual framing, the chapter then documents the different types of internet shutdowns that have been evolving in African countries over the past six years, from nationwide shutdowns of all internet traffic and mobile communications to more targeted geographical shutdowns or shutting down of a single social media platform. The chapter will also provide a brief historical overview of how authorities in Egypt, Guinea and other parts of the world resorted to shutdowns to silence dissent. Case studies from Ethiopia, Nigeria and Uganda provide context and allow us to analyse the causes and effects of internet shutdowns on digital citizenship. We then document the range of methods and strategies that citizens and civil-society organizations use to evade, mitigate and end internet shutdowns. The chapter concludes with recommendations arising from our analysis for how to end internet shutdowns and thereby increase the space for digital citizenship.

How internet shutdowns constrain digital citizenship

The ability to use mobile phones, internet communications and social media platforms has enhanced the speed, scale and scope of citizens' ability to organize and aggregate their voice to claim rights and otherwise participate in policy debates (DW 2018). For those able to access mobile and internet technologies, it has become possible to access and share information across borders, in some cases making it possible to bring global attention to a local rights issue. In their study of the impact of technology on citizen participation in local governance, Erete and Burrell (2017) point to the capacity to use digital technologies to heighten the visibility of citizens' concerns, to create novel spaces for participation in governance and to provide new mechanisms to call governments to account. However, they also point out that while communities may make effective use of digital technologies to raise issues, this does not necessarily increase their political power to have those issues resolved. Having a greater voice does not necessarily mean having greater power.

As in other parts of the world, governments across Africa are increasingly resorting to internet shutdowns as a means of control (Access Now 2021a). The Shutdown Tracker Optimization Project (STOP) run by the non-governmental organization (NGO) Access Now has documented more than 935 cases of intentional internet shutdowns in 60 countries globally from January 2016 to December 2021. Access Now documented a total of 118 internet shutdowns in 36 African countries between January 2016 and December 2021 (see Table 4.1). Ethiopia has shut down the internet twenty-two times, twice as many times as the next highest country (Algeria and Sudan, with eleven and ten shutdowns respectively), followed by Chad with seven and the Democratic Republic of Congo (DRC) with six shutdowns. During the same period, Benin, Burkina Faso, Burundi, Cameroon, Egypt, Eswatini (formerly Swaziland), Guinea,

Table 4.1 Incidence of Internet Shutdowns in Africa, January 2016 to December 2021

Number of shutdowns	**Countries**
22	Ethiopia
11	Algeria
10	Sudan
7	Chad
6	Democratic Republic of Congo
5	Cameroon, Egypt, Mali, Togo, Uganda
3	Nigeria, Gabon
2	Benin, Equatorial Guinea, Eswatini, Guinea, Kenya, Zimbabwe, Morocco,
1	Burkina Faso, Burundi, Côte d'Ivoire, Eritrea, The Gambia, Liberia, Libya, Malawi, Mauritania, Niger, Rep. of Congo, Senegal, Sierra Leone, South Sudan, Somalia, Tanzania, Zambia
118	**Total**

Source: Adapted from Access Now (2021) STOP Database. https://docs.google.com/spreadsheets/d/19uWafg_nDavtX_KpQAuTWp762s3yC6KeilkfLV5ZQeI/edit#gid=0

Liberia, Niger, Liberia, Republic of Congo, Mali, Togo and Uganda had also imposed internet shutdowns or social media blackouts. Although a majority of the shutdowns documented in Africa were ordered or perpetrated by state actors, it is important to note that shutdowns reported in countries such as Côte d'Ivoire (Reuters Staff 2018) and Kenya (Goldman, 2020; The Star 2020) were as a result of third-party attacks or actors.

Over the past years, authorities in Africa have shut down the internet and digital communication platforms during key national events, including elections, referendums, protests and conflict or communal violence, visits by government officials and inauguration ceremonies (Taye 2021). Countries such as Cameroon, Chad and Ethiopia have also imposed shutdowns lasting several months (and on occasion for more than a year). Elsewhere, internet shutdowns have been weaponized against minority groups or vulnerable communities, including refugees and displaced persons (Taye 2019). In the past, African governments tended to use nationwide shutdowns that affected all citizens and businesses, but by 2019, 20 per cent of Africa's internet shutdowns were sub-national and targeted specific districts or regions (Access Now 2021b).

Given the increasing centrality of digital communications to social, economic and political life, cutting off the internet comes at an enormous cost, to the economy, to personal lives and to human rights. Internet shutdowns prevent citizens from actively participating and contributing to social, economic and political life online. In this chapter, we show how internet shutdowns violate citizens' fundamental human rights to freely access information and exercise their freedom of association and speech. This builds on the work of Anthonio and Cheng (2021) and Mare (2020) who have highlight how internet shutdowns in Tanzania, Uganda and Zimbabwe have stripped citizens of their right to engage in the electoral process.

Conceptual framing

Citizenship is often understood in a narrow sense to refer to the legal status bestowed by the state on individuals. This legalistic conception of citizenship is certified with a national identity (ID) card or passport that confers rights and responsibilities. Understood in a broader sense, citizenship can describe a person's active engagement in social and political life, perhaps as a member of a school governance board, running a climate group or participating in elections. In a classic definition of citizenship, Marshall (1950: 14) describes citizenship as 'a status bestowed on those who are full members of a community'. This frames citizens as relatively passive recipients of a status by those with power to grant that status. Gaventa (2002) is among those who argue that to be meaningful, any conception of citizenship carries with it a conception of rights and entitlements. However, Nyamu-Musembi (2005) has pointed out that citizenship rights are rarely 'bestowed' upon excluded groups without active struggle for suffrage or equality. Her understanding of citizenship is 'based on the recognition that rights are shaped through actual struggles informed by peoples' own understandings of what they are entitled to'. This agency-based conception of citizenship as the active engagement of individuals in the political, economic and social life of their community (regardless of their legal status) is the one that we use in this chapter.

Building on this definition, *digital citizenship* is the process of active engagement in the civic life of a community using digital tools or online spaces. This may or may not involve participation in formal politics; however, not all online activity can be considered citizenship (take online gambling, for instance). Determining exactly what does and does not constitute digital citizenship is contested. At the most basic level, Mossberger, Tolbert and

McNeal (2008) define digital citizenship as the ability to participate (daily) in civic life online and to use mobile and internet tools in economic activity. Unlike citizenship, digital citizenship is not a status bestowed upon individuals; anyone with digital devices, connectivity and literacies can engage in civic life online. This may, for example, be by engaging with online communities, debates, petitions or hashtag campaigns. The case studies discussed in this chapter include examples of digital citizenship such as the #ENDSARS protest in Nigeria, claiming the right to freedom from police violence, and the #KeepItOn campaign against internet shutdowns, claiming the rights to online expression and communication. From this perspective, digital citizenship is understood not as a status but as an agency-based process of civic engagement and rights-claiming (Isin and Ruppert 2015: Hintz, Dencik and Wahl-Jorgensen 2019).

The concept of affordances is useful for understanding what it is about a particular technology that 'affords' a specific possibility for action. In this case, what is it about social media that affords us the possibility for viral campaigning or what is it about the internet 'kill switch' that affords a president the action possibility of a shutdown? Norman (1988) used the term 'affordances' to refer to the specific features of a technology that invite, facilitate or enable particular actionable possibilities. Hutchby (2001: 5) argues that affordances 'frame, while not determining, the possibilities for action in relation to an object' and provide us with a means for empirically analysing the 'effects' and 'constraints' associated with particular technologies. We will use the concept of affordances to understand the effects and constraints of the emerging range of new 'shutdown technologies' as well as the technologies of digital citizenship, including hashtags and virtual private networks (VPNs). First, we address some definitional issues before presenting a typology of different forms of internet shutdowns.

Defining internet shutdowns

The two most often quoted definitions of internet shutdowns are provided by Access Now (2021a):

> An internet shutdown happens when someone – usually a government – intentionally disrupts the internet or mobile apps to control what people say or do. Shutdowns are also sometimes called 'blackouts' or 'kill switches'.

And the more technical definition:

> An internet shutdown is 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.[1]

Typology of internet shutdowns

An internet shutdown can be a complete shutdown of all internet traffic nationwide. This was the original form of internet shutdown and remains the most common form. However, it can also take the form of a partial shutdown of a single website or of a specific district (Malik 2020). The recent Twitter ban in Nigeria is an example of only shutting down a specific social media platform. The internet shutdown in the Ethiopian region of Tigray at the time of writing is another example of a shutdown in a specific geography. The technology enabling more targeted shutdowns is becoming more sophisticated. States are now buying surveillance software that uses artificial intelligence with automated keyword search that can be used to target specific websites for shutdowns. Given the economic and political costs of nationwide shutdowns, we predict internet shutdowns will become more targeted over time.

Another way that governments repress digital dissent is by imposing mobile shutdowns, as recently reported in Niger, when authorities shut down mobile internet connection for ten days in response to post-election protests in the country (AFP 2021a). The impact of this form of internet shutdown is most effective in developing countries, where the vast majority of internet access is via mobile phones.

In 2019, 93 per cent of the sub-Saharan region was covered by a mobile phone signal, of which 75% included 3G and 50% included 4G mobile internet (Wyrzykowski 2020). In such cases, instructing the mobile phone companies to shut down removes internet connections from everyone except the small

[1] Access Now (2021) #KeepItOn FAQs.

percentage privileged to have domestic broadband connections. Mobile internet connectivity also affords the state the ‘action possibility’ of disrupting communications in ways that fall short of a shutdown. The technique of ‘throttling’, for example, enables states to slow internet speeds sufficiently to make digital citizenship on social media practically impossible, without completely shutting off the internet. This can be achieved by reducing the mobile connection from the fourth-generation service (4G) that allows us to use Twitter and TikTok on our phones back to the 2G service that only allows voice and SMS. By such means, governments can control the flow of information and silence dissenting voices. This is not only a violation of citizens’ constitutional and human rights to freedom of expression and freedom of information, but intentional internet shutdowns and disruption close down the space for digital citizenship. This is always illegal in international law:

> Filtering of content on the Internet, using communications ‘kill switches’ (i.e. shutting down entire parts of communications systems) and the physical takeover of broadcasting stations are measures which can never be justified under human rights law.
>
> Joint Declaration on Freedom of Expression and responses to conflict situations, 4c.
>
> (OHCHR 2015)

Governments resort to different tactics to shut down the internet. In most countries, private companies are responsible for implementing internet shutdowns that have been ordered by the state. The switch is operated by telecommunication service providers (telcos) and internet service providers (ISPs). These orders could be to shut down all services nationwide, to cut off a particular region, a particular social media platform, or to throttle services to make them practically useless.

For instance, in August 2019, authorities in India ordered ISPs to shut down the internet and all communications in the disputed region of Jammu and Kashmir (Masih, Irfan and Slater 2019). Access to landlines and 2G mobile phone calls were restored two months later but the 4G internet remained blocked, throttling internet speeds until full access was restored in February 2021 (Tiwary, Sharma and Iqbal 2021). The people of Jammu and Kashmir continue to experience intermittent internet shutdowns, with the most recent being ordered on 2 September 2021 following the death of the Kashmiri separatist leader Syed Ali Shah Geelani. India is the world's most frequent perpetrator of shutdowns, most often using targeted sub-national shutdowns that coincide with civic protest and digital citizenship (Mukhtar and Aafaq 2021).

An alternative to a full internet shutdown is to block particular websites or social media platforms, which is achieved when ISP companies block certain website addresses to make them inaccessible (Minges 2007). Governments are finding innovative ways to automate the implementation of these partial internet shutdowns through the use of artificial intelligence. The Israeli company Allot sells Deep Packet Inspection (DPI) technology, which can be used to intercept and block any content deemed 'harmful', and 'record detailed web activity logs' and control 'dangerous' traffic (Woodhams and O'Donnell 2021). Allot has provided the Tanzanian government with such internet filtering equipment that was used to intentionally disrupt access to Twitter, WhatsApp and Telegram before the election in October 2020 (Woodhams and O'Donnell 2021). These instances show not only that internet shutdowns are increasing but that governments are increasing spending on actions to disrupt citizens' right to information and communication during elections and popular protest (Tackett, Krapiva and Anthonio 2020). The increasing sophistication of more narrowly targeted shutdowns aids the ability of states to limit the violation of rights to smaller demographics. The examples also show that the ability of the state to violate human rights depends on the cooperation of private companies, both those that supply the surveillance and shutdown technologies and the telcos and ISPs that operate the kill switch.

Why and when do internet shutdowns happen?

Having explored the range of shutdown types, this section discusses when and why they happen: both in terms of justifications offered by governments and those suggested by critics.

Lewis (2021) argues that the internet and digital technologies are transforming society, business and politics as people respond to new opportunities online and change their behaviour accordingly. The internet and new media platforms such as Facebook, Twitter, WhatsApp and Signal have provided citizens with new means to effectively mobilize and participate in democratic discourse. Nabatchi and Mergel (2010) refer to this as Participation 2.0 and argue that internet and social media technologies have become essential tools allowing citizen engagement in governance at both national and local levels. They further intimate that in addition to the other benefits these platforms provide, they serve as a channel to facilitate 'open and transparent government, increase citizen trust and political efficacy, and improve the responsiveness of government to citizen needs and concerns'. Writing about the popular uprising across North Africa in 2011, Chatora (2012) shows how the use of the microblogging site Twitter, social networking site Facebook and mobile telephony played a key role in facilitating active political expression during the so-called Arab Spring that resulted in the ousting of Presidents Ben Ali (in Tunisia) and Mubarak (in Egypt). In her book *Twitter and Tear Gas*, Tufekci (2017) writes that Mubarak's government did not initially grasp the powerful affordances of social media that enabled the instant interactive nationwide communication used to mobilize and inform the popular uprising against continued rights violations by the state.

When Mubarak realized that digital citizenship threatened his hold on power, he implemented a full-scale internet shutdown drawing international condemnation and attention to the use of such repressive tactics to weaken digital citizenship. The Egyptian government intentionally cut off voice, SMS and social media functionality in an attempt to quell protests that were being coordinated partly by using digital tools (Marchant and Stremlau 2020). The first internet shutdown in Africa occurred in Zambia in 1996, and in both Guinea and Ethiopia in 2007, but it was the internet shutdown in Egypt during the 2011 Arab Spring that created global awareness of the phenomenon (Okunola 2018). These first internet shutdowns were also seminal acts of 'digital authoritarianism', in which the affordances of digital technologies are used by those in power to restrict citizens' freedoms and rights. Prior to the shutdown in Egypt, countries such as Iran had imposed internet shutdowns while authorities in Tunisia tightened its control online by censoring websites in response to protests (Jigsaw 2021). Since that time, internet shutdowns have become weaponized as a technological means to dampen dissent and to silence the public acts of rights-claiming that characterize digital citizenship (Ritzen 2021).

When states implement internet shutdowns, they do not say their intention is to violate the freedom of communication of political opposition or to disrupt the coordination of peaceful protest. In seeking to justify the use of internet shutdowns, governments cite diverse reasons, including the need to ensure 'national security and restore public order or for precautionary measures', to 'prevent the spread of misinformation or hate speech or illegal content' or 'to prevent cheating during school exams' (Internet Society 2019). In other instances, authorities do not provide any explanation as to why a shutdown is happening. However, shutdowns are frequently timed to coincide with elections or protests and have the effect of silencing digital citizenship and peaceful opposition. Taye (2021) has also shown the correlation between internet shutdowns and human rights violations carried out by the state. Her research cites incidents when shutdowns coincide with police and military operations against opposition groups. Shutdowns also make it difficult for journalists and activists to effectively document political activity and publish on time during important events (Rozen 2017).

Internet shutdowns can suppress the truth about human rights abuses committed by the state. Amnesty International's (2020) analysis of the five-day Iranian internet shutdown in November 2019 shows that more than 300 men, women and children were killed during the protests. The internet shutdown made it difficult for people to share information about what was happening, thereby obstructing research into the reported incidents of human rights violations. Human Rights Watch (2019) documented that during the month-long internet shutdown in Sudan imposed in response to peaceful protests in June 2019, state security forces killed at least 100 civilians. Rozen (2017) shows how internet shutdowns make it difficult for journalists to document and draw attention to human rights violations perpetrated by the state.

Some governments, including Bangladesh, India, Myanmar and Indonesia, have imposed internet shutdowns in order to silence voices of specific populations, such as members of oppressed or marginalized minority groups, refugees and others whose human rights are at risk (Taye 2019). In 2019, the authorities in Bangladesh shut down 3G and 4G mobile internet services in the Cox's Bazar refugee camps and its surroundings, which housed millions of Rohingyas who had fled Myanmar to avoid persecution and also made it illegal for refugees to get access to SIM cards (Human Rights Watch 2019). Similarly, in neighbouring Myanmar, the Ministry of Transport and Communication ordered all telecom service providers to shut down the internet in nine townships in Rakhine and Chin states in June 2019, amid violence and conflict (ARTICLE 19 2019).

India shut down the internet for 175 days in Jammu and Kashmir in response to protests following the government's introduction of legislation aimed at changing its political structure. The government also banned public gatherings, arrested local leaders and deployed thousands of troops to enforce the order. There were reports of heinous human rights violations reported in Kashmir perpetrated by government forces including arbitrary arrests and physical assaults against Kashmiris including children as young as nine years (Ghoshal et al.).

It is sometimes argued that internet shutdowns and state violence go hand in hand. Gohdes (2015) analysed the daily record of documented state killings during the Syrian civil war and noted that internet shutdowns correlate with 'significantly higher levels of state repression, most notably in areas where government forces are actively fighting violent opposition groups'. She adds that communication blackouts are a tactic of war designed to decrease opposition groups' capabilities to successfully coordinate and implement attacks against the state, giving regime forces time to strengthen their position. Gohdes's research shows that internet shutdowns are used to weaken opposition groups' capabilities to coordinate and mobilize online. This highlights both the affordances of digital technologies for enabling civic mobilization and the affordances of state shutdowns for repression.

Analysis across these examples shows that internet shutdowns do not happen in isolation. Before a shutdown is imposed, there is usually a trigger such as street demonstrations or online protests, upcoming elections or 'security operations'. In authoritarian settings, digital citizenship can be perceived as a threat to the interests of powerholders who sometimes use internet shutdowns to extinguish its threat. Internet shutdowns are often either a reaction to government opposition or a proactive step to pre-empt opposition. Repressive states often impose internet shutdowns when they fear that digital citizenship is a threat to their interests and hold on power. Put most succinctly, internet shutdowns are designed to constrain digital citizenship.

Internet shutdowns violate human rights

The legal basis for the right to unrestricted internet communication could not be clearer. Article 19 of the Universal Declaration of Human Rights

(United Nations Office of the High Commissioner for Human Rights 1966) states that ‘Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers’. This fundamental human right is guaranteed to all citizens and was given legal force by the International Covenant on Civil and Political Rights in 1976 (United Nations 1967). In 2012, the UN Human Rights Council (UNHRC) unanimously passed a resolution on the promotion, protection and enjoyment of human rights on the internet, which ‘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, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights’ (UNHRC 2012). As part of the formal decolonisation process at the point of political independence, most African nations explicitly wrote freedom of information and communication into their new constitutions and subsequently codified those rights into domestic law (Roberts and Mohamed Ali 2021). Despite these strong legal foundations, the number of internet shutdowns violating citizens’ rights continues to increase.

The justifications that states provide for internet shutdowns often are not credible in law. International law makes it clear that it is only possible for a state to violate fundamental human rights in instances that are ‘legal, necessary and proportionate’. A state can pass a law that prescribes limited circumstances in which an individual’s right can be violated in order to prevent a greater evil. International law requires that the ‘legitimate aims’ of rights violations must be stipulated in law, and must be necessary and proportionate in scope to the harm being averted. The United Nations asserts that any restrictions to online expression must be strictly necessary and proportionate to achieve a legitimate function, stating that any ‘restrictive measures must . . . be the least intrusive instrument amongst those which might achieve their protective function; they must be proportionate to the interest to be protected’ (UNHRC 1999).

Internet shutdowns are never proportionate. They violate the human rights of all citizens, not only those suspected of committing the most serious crimes. The UN Special Rapporteur has denounced internet shutdowns as a violation of international human rights law, which cannot be justified under any circumstances (UN General Assembly, Human Rights Council 2021). The Special Rapporteur on the rights to freedom of peaceful assembly and association reaffirmed his concern, expressed in 2019, that 'network disruptions amid peaceful assemblies' have 'become a dangerous global trend'. The report stated that 'shutdowns are lasting longer, becoming harder to detect and targeting particular social media and messaging applications and specific localities and communities' (UN General Assembly, Human Rights Council 2021).

As explained earlier, although internet shutdowns are ordered by the state, they are carried out by private companies, internet service providers (ISPs) and mobile phone companies. This makes private companies complicit in human rights violations. Companies have clear obligations with regard to human rights violations. The United Nations Guiding Principles on Business and Human Rights (OHCHR 2011) and the OECD (2011) Guidelines for Multinational Enterprises clearly state the obligation of companies to respect human rights, prevent or mitigate potential harms and provide remedy for harms they cause or contribute to. Where civil society finds it impossible to put pressure on governments to end internet shutdowns, they may have more leverage putting pressure on the companies that operate the kill switch by demanding that they fulfil their obligations to protect human rights.

Given the increased use of internet shutdowns around the world, a number of regional and international efforts have been undertaken by diverse actors to bring an end to this increasing threat to democratic values and principles. In its thirty-second session, the United Nations Human Rights Council recognized the centrality of access to the internet to citizenship and called on all nations to promote and protect the enjoyment of human rights, including the right to freedom of opinion and expression, on the internet and using other information and communication technologies (ICTs), noting that the 'Internet can be an important tool for fostering citizen and civil-society participation, for the realisation of development in every community and for exercising human rights'. The United Nations expressed deep concern about measures aiming to or that intentionally prevent or disrupt access to or dissemination of information online, in violation of international human rights law' (UN 2016: 4). Similarly, the African Commission on Human and Peoples' Rights (2016) passed a resolution condemning the use of internet shutdowns by state parties during elections and protests. The Freedom Online Coalition (FOC), which was set up in 2017 and constitutes thirty governments, continues to declare its commitment to fighting internet shutdowns through periodic statements.

The next sections examine case studies from Ethiopia, Nigeria and Uganda to provide greater empirical depth to our analysis of internet shutdowns and digital citizenship.

Ethiopia

Ethiopia has implemented more internet shutdowns than any other country in Africa. Since 2016, authorities have imposed a series of shutdowns at national and sub-national scale, in order to quash protests or in response to communal violence or conflict. Seven national internet shutdowns were imposed while the remaining fifteen affected one or more regions during the monitoring period. At the time of writing (August 2022), the most recent shutdown which started on 4 November 2020 in the Tigray region and later affected the Afar and Amhara regions following the spread of the conflict had been ongoing for nearly two years. This case study highlights how authorities in Ethiopia use internet shutdowns to repress freedom of speech and to cover up violence perpetrated during peaceful protests and episodes of conflict.

In Ethiopia's north-west region of Tigray, conflict broke out between the federal government and the Tigray People's Liberation Front (TPLF) in 2020. An internet shutdown has effectively cut off the region from the rest of the world, disrupting reporting on human rights abuses being perpetrated against the civilian population. Both warring parties claim the other side is responsible for the communication blackout. In a statement issued by the state-owned Ethio Telecom, accusations were levelled against the TPLF, accusing them of intentionally destroying the phone and internet communication infrastructure in Tigray (Addis Fortune 2020). There have been reports of egregious human rights violations being carried out against Tigrayan civilians, including mass rape, mass murder and violent abuse of refugees by forces from Ethiopia and Eritrea (Debotch 2021). Testimonies collected show how the ongoing internet shutdown is making it difficult for families in and outside the region to stay connected and sustain their livelihoods (Access Now 2021a). Anna (2021) reports that the communication blackout has made it extremely difficult for journalists to cover what is taking place, while humanitarian aid workers are unable to access parts of the Tigray region and provide support for displaced persons and refugees (Parker 2021). Shutting down complete access to the internet and telecommunications during armed conflict contributes to further harm and endangers more lives. The current shutdown in Tigray is making it difficult for people fleeing the region to find safe havens (Dewaal 2021).

This is not the first time the internet has been shut off in parts of Ethiopia during armed conflict. In January 2020, the authorities disconnected telecommunications and internet services in several parts of western Oromia (Corey-Boulet 2020). The shutdowns happened amid reports of government military operations against the armed wing of the Oromo Liberation Front (OLF), which was once banned in the country (Aljazeera 2018). Corey-Boulet (2020) reported widescale human rights violations, including murder and mass detentions by government security forces, which were documented at the time. Again, in June 2020, authorities imposed a nationwide internet blackout that lasted over two weeks in response to protests following the murder of Oromo musician and social activist Hachalu Hundessa, who was shot dead in the capital, Addis Ababa (Access Now 2020).

Nigeria

Nigerian citizens are making increasing use of the mobile internet and social media applications (apps) to make demands on the government and to claim their rights. The number of social media users in Nigeria was estimated to be twenty-eight million in 2020 (Statista.com 2021). Social media apps have been used to enhance citizens' voice on issues that were not given prominence in traditional media outlets. Ajisafe, Ojo and Monyani (2021) argue that social media has reduced dependency on establishment media and has given people the opportunity to obtain and share information through unmediated communication channels. Nigeria experienced a surge in social media usage in recent years (Statista.com 2021), which has benefited social movements and expanded the space for digital citizenship.

The rise of the #ENDSARS movement in 2020 (explored in more detail in the Nigeria chapters) is a case in point. The off and online campaign called for the country's Special Anti-Robbery Squad (SARS) to be disbanded. The notorious police unit stands accused of systematic human rights violations.

The online campaign went viral internationally, amplified by Nigerians in the diaspora. Obia (2020) argues that the way in which the #ENDSARS protests were coordinated provides insights into how Twitter serves as a coordinating platform for oppositional discourse and activism in Nigeria. Kazeem (2020) also highlights how youth in Nigeria leveraged Twitter to organize online and off.

On 4 June 2021, authorities in Nigeria banned Twitter, making it inaccessible across the country without specialist circumvention tools. The immediate trigger for the ban was the company's deletion of a tweet posted by Nigeria's president Muhammadu Buhari. However, activists believe that the president's motives included silencing the online dissent of millions who rely on Twitter as a platform for their digital citizenship (Asadu 2021). Despite threats by the government to prosecute anyone who attempted to violate the ban, many Nigerians circumvented it by using VPNs to access the censored platform. Several civil-society organizations inside and outside of the country also challenged the legality of the ban in local and regional courts. A number of lawsuits were lodged against Nigeria's Twitter ban in the ECOWAS Court, the Community Court of Justice for the Economic Community of West African States. These lawsuits have since been merged into a single filing and are pending adjudication (Silas 2021).

Uganda

A few days before elections scheduled for 14 January 2021, authorities tightened control of Uganda's off and online civic space. Amid reports of a crackdown on dissidents and opposition politicians, the Uganda Communications Commission (UCC) ordered the country's ISPs to implement a partial shutdown by blocking access to specific social media apps, including Facebook, Twitter, WhatsApp, Instagram and Google Play Store (Kafeero 2021). The authorities also blocked access to several VPNs in an attempt to prevent circumvention of the shutdowns. On the eve of elections, the government ordered a complete internet blackout, leaving millions of people in digital darkness. The shutdown made it impossible for Ugandans to access information about the election process, to freely express themselves or to stay in touch with their families (Anthonio 2021). Ugandans were unable to engage in online commerce in the absence of essential services such as mobile payment services and internet banking, with unquantified costs to local businesses. The government justified the four-day internet shutdown as a 'national security' measure (AFP 2021b). However, Facebook remained blocked almost a year later. General Museveni, who captured power in 1986, said in a televised state broadcast that he had blocked Facebook in response to the company's suspension of pro-government accounts for their 'coordinated inauthentic behaviour' – a term used to refer to the activity of actors designed to covertly manipulate online debate (Facebook 2021).

This was not the first internet shutdown during elections in Uganda. On 18 February 2016, authorities shut down social media platforms and mobile transaction services during the presidential elections. Internet users could not access platforms such as Facebook, Twitter, WhatsApp and other communication tools unless they had circumvention tools. The Associated Press (Muhumuza and Curtis 2016) reported that according to the UCC, the shutdown was imposed following orders from the Electoral Commission for 'security reasons'. At that time, President Museveni admitted to the media that he had ordered the shutdown because 'steps must be taken for security to stop so many [social media users] from getting in trouble; it is temporary because some people use those pathways for telling lies'. The shutdown lasted four days. In May of the same year, during President Museveni's inauguration ceremony, authorities ordered ISPs to shut down social media platforms for 'national security reasons' (Nanfuka 2016). Prior to the social media shutdown, authorities banned live media coverage of opposition-led activities as they protested against what they considered as yet another rigged election. During the same period, journalists and artists had decried the deteriorating state of freedom of expression in the country (Kalemera 2016).

In November 2016, Unwanted Witness Uganda, a civil-society organization, filed two lawsuits in Uganda's High Court and Constitutional Court against the government and ISPs who implemented the social media blackouts. They argued that the internet shutdowns violated fundamental human rights and contravened national, regional and international legal frameworks. The case, which had been delayed for several years, is back on the agenda of the courts but is still awaiting a judgement. After the January 2021 shutdown, Unwanted Witness (2021) again filed a court petition urging the court to prevent the government and ISPs from imposing future arbitrary and unjustified internet shutdowns in violation of human rights.

How are citizens acting to recover their digital citizenship?

As noted in the aforementioned case studies, citizens are not passive in the face of the human rights violations that internet shutdowns present. They are using a range of tactics to reassert digital citizenship by circumventing or challenging internet shutdowns. This includes technical, legal and political tactics. Technical circumvention tools such as VPNs anonymized web browsers like Tor or messaging apps like Signal, and mesh networks enable citizens to technically bypass surveillance and internet shutdowns. Also, monitoring and advocacy campaigns like the #KeepItOn campaign[2] fight internet shutdowns globally. The following sections discuss the various ways governments shut down the internet – and highlight main tools available to counter the different types of internet shutdowns currently experienced.

Technical tools to overcome shutdowns

Partial shutdowns: When shutdowns affect specific platforms, circumvention tools like VPNs are useful to enable citizens to continue accessing the blocked applications. VPNs allow individuals to redirect their internet connection through a remote server in another country to bypass the internet shutdown in their own country. By this means, Ugandans can pretend to be logging on from Kenya and circumvent a partial shutdown in Uganda. In most cases, VPNs also add a layer of security and privacy to protect against surveillance. Although the use of VPNs has increased exponentially, some countries like Tanzania, Uganda and the regional government in Jammu and Kashmir in India have cracked down on the use of VPNs and other tools for security, anonymity and

[2] A global campaign that unites over 240 organizations around the world using a wide range of approaches to challenge internet shutdowns, including grassroots advocacy, direct policymaker engagement, technical support, corporate accountability and legal intervention. https://www.accessnow.org/keepiton/

circumvention, such as those from the Tor Project. The government of Belarus has blocked VPN providers and the Tor site since 2015.

Throttling: This term refers to the intentional slowing down of internet speeds or bandwidth to make it difficult to upload or download content (Surfshark 2020). Throttling is an artificial restriction, but not entirely stopping, of the flow of data through a communications network. This means that internet access may seem available but not usable due to the interference (Björksten 2022). This type of shutdown is often difficult to identify or detect as it can be attributed to a poor internet connection. However, users can accurately detect throttling by running online speed tests and installing VPNs or proxies to encrypt their location and reroute their connection. To run an effective speed test, it is important to first run the test without a VPN and then with a VPN installed. This allows users to compare and analyse local internet speeds.

Complete internet shutdown: Also known as a 'blackout' or 'kill switch', this occurs when internet access drops to near-zero. The technical impact of a complete shutdown can extend beyond borders and threaten the global internet infrastructure**.** Circumventing complete internet shutdowns remains a challenge for both technical and non-technical actors. A number of tactics are currently employed, as described here:

> **Use of satellite dishes**: Independent satellite connections can be used to circumvent ISP connections and provide an alternative means of accessing information during a complete shutdown. For instance, Iranians in the diaspora launched Toosheh, or 'Knapsack', a satellite file-casting app that aggregates uncensored digital content, like news articles, YouTube videos and podcasts, and makes them available via satellite TV to locations otherwise disconnected due to remote geography, internet shutdowns or high costs (Net Freedom Pioneers 2016). This technology is currently in use in Iran and the Middle East. It is advisable for users to download the app ahead of time to allow the satellite transfers to circumvent the internet shutdown entirely.
>
> **Mesh networks**: Mesh networks allow users to tap into radio frequencies to access connectivity during full internet shutdowns. Mesh network services mostly rely on Bluetooth, allowing users to communicate through a network

of devices that are linked locally, rather than over an internet connection. The FireChat mesh network, which uses wireless mesh networking to enable smartphones to connect via Bluetooth or WiFi without an internet connection, was also used during Hong Kong's democracy protests in 2014 (Sruthijith 2014). More recently, the Bridgefy app and software development kit have been introduced, which allow for offline text messages to be sent via Bluetooth when there is no access to the internet, making it possible to keep lines of communication open during complete shutdowns. In response to a potential shutdown threat during the 2019 pro-democracy demonstrations in Hong Kong, protesters began downloading mesh networks, and Bridgefy soared in popularity during the aftermath of the 2021 coup in Myanmar (Jigsaw 2021).

Use of international SIM cards with roaming services: Another way to circumvent internet shutdowns is the use of foreign mobile SIM cards or travel to neighbouring countries or regions in order to access the internet. The use of SIM cards from neighbouring countries was a common tactic among activists in Sudan during the 2019 internet shutdown (Hamad 2020). Sudanese citizens resorted to using SIM cards from India, Saudi Arabia, Egypt and the United Arab Emirates. When authorities became aware of this tactic, they disabled the roaming feature on cellular data networks.

Although use of satellites is expensive and the use of foreign SIM cards is insecure, they are the most common tools currently used in African countries to bypass complete internet shutdowns. There is a need for further research and investment in public awareness by civil-society actors and the media to enable people to freely and safely bypass complete internet shutdowns and restore their right to free speech and association.

Non-technical means of advocating against internet shutdowns

It is vital that civil society can continue monitoring, documenting, analysing and raising awareness about internet shutdowns through global coordinated efforts such as the #KeepItOn campaign. Advocacy work to disseminate information about technical circumvention is critical to enable people to exercise digital citizenship. Creating global awareness about state abuse of human rights is also vital to dissuade future internet shutdowns. This section looks at how civil-society groups and individuals have used strategic litigation to challenge and bring an end to internet shutdowns in both regional and national courts in Africa:

Strategic litigation

Citizens and activists around the world are increasingly resorting to courts to challenge internet shutdowns (Micek and Libbey 2019). A recent ruling by the Zambian High Court, for example, ordered President Edgar Lungu's government to restore internet services that had been blocked on 12 August, which was election day (New Zimbabwe 2021). The lawsuit was filed by a civil-society activist against the government. Most African nations have strong legal protections for unrestricted private communications, making this a potentially fruitful avenue of resistance in some countries (Roberts and Mohamed Ali 2021).

For the second time within two years, the Community Court of Justice of the Economic Community for West African States (ECOWAS Court) has declared internet shutdowns to be unlawful and in violation of fundamental rights. After several months of civil-society organisations both locally and internationally fighting the Nigerian government in court for shutting down microblogging application, Twitter for over seven months, the ECOWAS Court on July 14, 2022 ruled that the Twitter ban in Nigeria was unlawful and ordered the government to pay litigation fees of plaintiffs. The ECOWAS Court also held that the shutdown contravened both the African Charter on Human and Peoples' Rights and the United Nations Charter, and ordered the Nigerian government to take appropriate legislative steps to guarantee the rights of the plaintiffs (Media Rights Agenda 2022).

Similarly, the ECOWAS Court passed a landmark judgement in June 2020 upholding the right of freedom of expression in Togo and other African states in a lawsuit filed by local civil-society groups, with support from other regional and international NGOs. The ruling, which was in response to the Togolese government's decision to shut down the internet during anti-government protests in 2017, indicated that the shutdown was illegal, and the court cautioned the government not to repeat its action (Hughes 2020). The Court ruled that the shutdowns were imposed were in violation of fundamental human rights and that the government's justification for disrupting the internet in response to 'national security' arguments was unpersuasive, and insufficient under local or international law.

Over the years, activists and individuals in Sudan have leveraged national courts in response to the uptick in the use of internet shutdowns imposed by Sudanese authorities. There have been at least four court decisions against shutdowns in Sudan since 2019. Most recently, the Sudanese Consumer Protection Organization sued the Telecommunication and Post Regulatory Authority (TPRA) for shutting down the internet in October 2021. The presiding judge subsequently ordered access to be restored on November 11, 2021 (Reuters 2021). The TPRA argued against the restoration on the grounds of 'national security' and a 'state of emergency', arguments the court dismissed. The judge took an unprecedented step of issuing an arrest warrant for the chief executive officers of the telecom companies due to their failure to restore internet access. That is when access was finally restored. In an unrelated case, a Sudanese court in 2019 ordered mobile operator Zain Sudan to restore internet services after access was cut off to quell protests in the country. The case was filed by an individual lawyer, Abdel-Adheem Hassan, who filed his case against Zain Sudan over the military-ordered blackout. Internet access was subsequently restored across the country following the ruling. (Abdelaziz et al. 2019)

In Zimbabwe, civil-society activists successfully sued the state for shutting down the internet in 2019 during planned protests (Associated Press 2019). In a landmark decision, the court ruled that the Minister of State in the President's Office Responsible for National Security 'does not have the authority to issue any directives in terms of the Interception of Communications Act', making the order that led to the Zimbabwean internet shutdown illegal and without effect. (MISA-Zimbabwe 2019)

Although the use of litigation has not brought a complete end to the fight against internet shutdowns, it has contributed significantly to holding governments accountable and in setting precedents to deter others from normalizing the use of internet shutdowns. It is important for civil-society actors to remain resilient in the fight against shutdown legally at national, regional and even international levels.

Conclusion

This chapter has shown that digital citizenship can stimulate repressive governments to impose internet shutdowns and that internet blackouts can close down the space for digital citizenship. Internet shutdowns are a reflection both of the strength of authoritarian governments and of their fragility. That presidents fear online activity sufficiently to shut down the infrastructure of social, economic and political life is a testament to the growing strength of digital citizenship. Citizens have used online spaces creatively to exercise digital citizenship and are now innovating workarounds to internet shutdowns so that they continue to do so.

The cases presented in this chapter highlight concerns raised by civil-society groups around the world. The frequency of shutdowns is increasing, and they are lasting longer. The technologies of shutdowns are becoming more sophisticated, more targeted, harder to detect and as such may become extremely difficult to end the practice of internet shutdowns completely or draw less criticism to the issue. However, this in no way reduces the impact on those citizens whose rights are violated. Internet shutdowns cut off citizens and businesses, constraining livelihoods, education, family relationships and people's ability to take part in social, economic and political life. All individuals have a right to take part in open debate and decision-making on issues that affect their lives or call attention to human rights abuses being carried out by the state.

Internet shutdowns are evidence of the growing power of digital citizenship. Repressive governments are evidently threatened by the enhanced power and voice that use of digital technologies gives citizens. Regimes pay a political and economic cost when they shut down the internet, and they must expect to face domestic and international criticism and reduction in support. For this reason, internet shutdowns are perhaps easier to sustain in African countries where a relatively small percentage of the economy is online and political opposition is relatively weak. If this holds true, then, as economies increasingly move online and the economic costs of internet shutdowns grow, we should expect increased use of more narrowly targeted shutdowns and platform-specific measures like Nigeria's recent seven-month-long Twitter ban which was imposed by authorities on 4 June 2021.

To end the rights violations that internet shutdowns represent, it is necessary to bring irresistible pressure on states and on private mobile and internet service providers to end the practice. While the use of VPNs, satellite connectivity and mesh networks are valuable tactical responses that relieve the symptoms of this problem, the solution must be to make it politically untenable to impose shutdowns in the first place, through adoption of rights-respecting legislation, strategic litigation, electoral politics and advocacy – including by means of digital citizenship.

All internet shutdowns are a violation of human rights. The use of internet shutdowns is one weapon in the wider arsenal of digital authoritarianism. This chapter has shown how citizens experience internet shutdowns as a violation of human rights, as a silencing of their freedom of expression and as a curtailment of their ability to exercise, defend and claim fundamental human rights. Addressing these attacks on fundamental freedoms requires urgent action by all relevant actors, including national and foreign governments, private corporations, regional and international blocks, media outlets and civil-society groups.

Arising from the analysis in this chapter, we propose the following recommendations for policy, practice and further research.

Recommendations

The fight to end internet shutdowns to enable citizens to enjoy the full benefits of the internet and digital applications requires collective action by all parties. Here, we present a number of recommendations directed at regional and international organizations, governments, the private sector and civil society on how to strengthen the fight against internet shutdowns.

National governments should adopt human rights–centric legislation that refrains them from imposing internet shutdowns during important national events.

The international community should denounce the use of shutdowns increasingly and promptly as a violation of fundamental human rights and caution authorities to stop imposing them at all times. Additionally, international cooperation and aid institutions that seek to expand connectivity must include explicit references to preventing shutdowns in their licensing agreements. Companies and businesses must push back against internet shutdowns and undertake human rights due diligence with regard to potential adverse impacts from network shutdowns when entering or renegotiating licence agreements with governments at all levels. Finally, civil-society actors, academia and individuals must continue to work together through global initiatives like the #KeepItOn campaign to monitor, document and respond to shutdown threats around the world.

Bibliography

Abdelaziz, K (2019) 'Sudan Court Orders Company to End Military-Ordered Internet Blackout: Lawyer', Reuters website. https://www.reuters.com/article/us-sudan-politics-internet-idUSKCN1TO0FV.

Abrougui, A. (2021) 'Internet Shutdowns and Election Handbook', *Access Now*, 31 March, accessed 17 October 2021.

Access Now (2016) 'No More Internet Shutdowns! Let's #KeepItOn', accessed September 2021.

Access Now (2020) 'Back in the Dark: Ethiopia Shuts Down Internet Once Again', 16 July, accessed October 2021.

Access Now (2021a) 'Voices from Tigray: Ongoing Internet Shutdown Tearing Families, Communities, Businesses Apart', 13 September, accessed 17 October 2021.

Access Now (2021b) 'What's Happening in Tigray? Internet Shutdowns Avert Accountability', 29 July, accessed 17 October 2021.

Addis Fortune (2020) 'Ethio Telecom Claims Regional Operations in Meqelle Tampered With', 10 December, accessed 17 October 2021.

AFP (2021b) 'Uganda Eases Internet Shutdown Imposed over Election', *France 24*, 18 January, accessed September 2021.

African Commission on Human and Peoples' Rights (2016) '362 Resolution on the Right to Freedom of Information and Expression on the Internet in Africa', accessed 17 October 2021.

African School on Internet Governance (2016) 'Statement on Intentional Internet Shutdowns', accessed 17 October 2021.

Agence France Presse (AFP) (2021a) 'Internet Back in Niger After Post-Election Blackout', *The Guardian Nigeria*, 6 March, accessed 17 October 2021.

Ajisafe, D., A. Ojo, and M. Monyani (2021) 'The Impacts of Social Media on the #EndSARS# Youth Protests in Nigeria', in *Proceedings of the International Conference of Information Communication Technologies Enhanced Social Sciences and Humanities (ICTeSSH) 2021 Conference*, accessed 17 October 2021.

Aljazeera (2018) ‘Thousands of Ethiopians Hail Return of Once-Banned Oromo Group’, 15 September, accessed 17 October 2021.

Amnesty International (2020) ‘A Web of Impunity. The Killings Iran’s Internet Shutdown Hid’, accessed 17 October 2021.

Anna, C. (2021) ‘“We’ll Be Left Without Families”: Fear in Ethiopia’s Tigray’, *AP News*, 11 February, accessed 17 October 2021.

Anthonio, F. (2021) ‘“No Matter What They Do, The World Is Watching”: Some Ugandans Are Back Online After Internet Shutdown During Presidential Election’, *Access Now*, 20 January, accessed 17 October 2021.

Anthonio, F. and S. Cheng (2021) ‘Cutting Internet Access When People Need It the Most: Stories from Uganda’, *Access Now*, 9 February, accessed 17 October 2021.

Asadu, C. (2021) ‘Nigeria’s Twitter Blackout: What’s Really Behind Buhari’s Social Media Ban?’, *Nigeria, The Africa Report*, 7 June, accessed 17 October 2021.

Associated Press (2019) ‘Zim High Court Rules Internet Shutdown Illegal, Orders Govt to Restore Full Internet to the Country’, *Harare, News24*, 21 January, accessed 17 October 2021.

Best, M. and A. Meng (2015) ‘Twitter Democracy: Policy Versus Identity Politics in Three Emerging African Democracies’, in *Proceedings of the Seventh International Conference on Information and Communication Technologies and Development*, accessed October 2021.

Björksten, G. (2022) ‘A Taxonomy of Internet Shutdown: The Technologies Behind Network Interference’, *Access Now*, 1 June, accessed 14 August 2022.

Bridgefy (2020) ‘How Does the Bridgefy App Work?’, accessed 17 October 2021.

Chatora, A. (2012) *Encouraging Political Participation in Africa: The Potential of Social Media Platforms*, Pretoria: Institute for Security Studies, accessed 17 October 2021.

Corey-Boulet, R. (2020) ‘Ethiopia’s Abiy Faces Outcry over Crackdown on Rebels’, *AFP*, 29 February, accessed August 2021.

Debotch, R. (2021) ‘Vicious Mass Rape of Women Has Become a Weapon Against the Tigray in Ethiopian War’, *Global Voices*, 5 July, accessed 17 October 2021.

Dewaal, A. (2021) ‘Switch Tigray’s Internet Back On, World Peace Foundation’, 21 April, accessed September 2021.

DW (2018) ‘How the Internet Changes Political Debate’, *DW*, 29 June, accessed August 24, 2022.

ECOWAS Community Court of Justice (2020) ‘Economic Community for West African States (ECOWAS) Community Court of Justice Ruling’, 25 June, accessed 17 October 2021.

Erete, S. and J. Burrell (2017) ‘Empowered Participation: How Citizens Use Technology in Local Governance’, in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*.

Facebook (2021) 'What Does Coordinated Inauthentic Behaviour Mean?', 6 December, accessed 17 October 2021.

Flores, W. and R. Benmayor (1997) *Latino Cultural Citizenship: Claiming Identity, Space and Rights*, Boston: Beacon Press.

Freedom Online Coalition (2017) 'Joint Statement on State Sponsored Network Disruptions', accessed July 2021.

Freedom Online Coalition (2021) 'FOC Issues Joint Statement on COVID-19 and Internet Freedom', 27 May, accessed 17 October 2021.

Gaventa, J. (2002) 'Exploring Citizenship, Participation and Accountability', *IDS Bulletin*, 33 (2): 1–14, accessed 17 October 2021.

Gohdes, A. (2015) 'Pulling the Plug: Network Disruptions and Violence in Civil Conflict', *Journal of Peace Research*, 52 (3): 352–67, accessed July 2021.

Goldman, D. (2020) 'Agent Saboteurs Within Somalia Army Jam Kenya's Safaricom BTS-Mast in Mandera Frontier', *Strategic Intelligence*, 2 March, accessed 24 August 2022.

Guest, P. (2022) 'In the Dark: The Internet Sparked a Revolution, Then It Was Turned Off', *Rest of World*, 22 April, accessed 14 August 2022.

Hamad, K. (2020) 'Internet Shutdowns in Sudan: The Story Behind the Numbers and Statistics', *Global Voices*, 8 June, accessed 17 October 2021.

Hintz, A., L. Dencik, and K. Wahl-Jorgensen (2019) *Digital Citizenship in a Datafied Society*, Cambridge: Polity Press.

Hughes, P. (2020) 'Landmark Judgment: ECOWAS Court Finds Togo Violated FoE with Internet Shutdown', *Media Defence*, 25 June, accessed 17 October 2021.

Human Rights Watch (2019) 'Sudan: End Network Shutdown Immediately', 12 June, accessed 17 October 2021.

Hutchby, I. (2001) 'Technologies, Texts and Affordances', *Sociology*, 35 (2): 441–56.

Internet Society (2019) 'Policy Brief: Internet Shutdowns', accessed August 2021.

Isin, E. and E. Ruppert (2015) *Being Digital Citizens*, London: Rowman & Littlefield.

Isin, E. and P. Wood (1999) *Citizenship and Identity, Politics and Culture Series*, London: Sage Publications.

Jigsaw (2021) 'The Internet Shutdowns Issue', *The Current*, accessed 17 October 2021.

Jones, E. and J. Gaventa (2002) *Concepts of Citizenship: A Review*, Brighton: Institute of Development Studies, accessed 17 October 2021.

Kabeer, N. (2005) *Inclusive Citizenship: Meanings and Expressions*, London: Zed Books.

Kafeero, S. (2021) 'Uganda Has Shut Down All Social Media Two Days Ahead of a Tense Election', *Quartz Africa*, 12 January, accessed 17 October 2021.

Kalemera, A. (2016) 'Ugandan Artists, Journalists Decry Declining Freedom of Expression', *CIPESA*, 5 May, accessed 17 October 2021.

Kazeem, Y. (2020) 'How a Youth-Led Digital Movement Is Driving Nigeria's Largest Protests in a Decade', *Quartz Africa*, 13 October, accessed 17 October 2021.

Lewis, J. (2021) 'A Short Discussion of the Internet's Effect on Politics', *Centre for Strategic and International Studies*, 29 January, accessed 14 August 2022.

Lister, R. (2003) *Citizenship: Feminist Perspectives*, London: Palgrave Macmillan.

Malik, I. (2020) 'A Year Without High-Speed Internet Has Been a Nightmare for J&K's Entrepreneurs', *The Wire*, 2 August, accessed 17 October 2021.

Marchant, E. and N. Stremlau (2020) 'The Changing Landscape of Internet Shutdowns in Africa', *International Journal of Communication*, 14 (1): 4216, accessed September 2021.

Mare, A. (2020) 'Internet Shutdowns in Africa| State-Ordered Internet Shutdowns and Digital Authoritarianism in Zimbabwe', *International Journal of Communications*, accessed September 2021.

Marshall, T. (1950) *Citizenship and Social Class*, Cambridge: Cambridge University Press.

Masih, N., S. Irfan, and J. Slater (2019) 'India's Internet Shutdown in Kashmir Is the Longest Ever in a Democracy', *Washington Post*, 16 December, accessed 17 October 2021.

Media Rights Agenda (2022) 'Media Rights Agenda, Others Win Suit over Twitter Ban as ECOWAS Court Rules Nigerian Government's Action Unlawful', Media Rights Agenda website. https://mediarightsagenda.org/media-rights-agenda-others-win-suit-over-twitter-ban-as-ecowas-court-rules-nigerian-governments-action-unlawful/.

Micek, P. and M. Libbey (2019) 'Judges Raise the Gavel to #KeepItOn Around the World', *Access Now*, 23 September, accessed 17 October 2021.

Minges, M. (2007) *Mobile Internet for Developing Countries*, Geneva: International Telecommunication Union.

MISA Zimbabwe (2019) 'High Court Sets Aside Internet Shutdown Directives', Media Institute for Southern Africa website. https://zimbabwe.misa.org/2019/01/21/high-court-sets-aside-internet-shut-down-directives/.

Mossberger, K., C. J. Tolbert, and R. S. McNeal (2008) *Digital Citizenship: The Internet, Society, and Participation*, Cambridge, MA: MIT Press.

Muhumuza, R. and B. Curtis (2016) 'Voting in Uganda Plagued by Delays; Social Media Shut Down', *Global News*, 18 February, accessed September 2021.

Mukhtar, U. and Z. Aafaq (2021) '"It Is Humiliation for Us": Internet Shutdown Blocks News in Kashmir', *The Wire*, 2 September, accessed 17 October 2021.

Nabatchi, T. and I. Mergel (2010) *Participation 2.0: Using Internet and Social Media Technologies to Promote Distributed Democracy and Create Digital Neighborhoods*, accessed August 2021.

Nanfuka, J. (2016) 'Uganda Again Blocks Social Media to Stifle Anti-Museveni Protests', 12 May, accessed September 2021.

Net Freedom Pioneers (2016) 'Empowering Offline Communities Anywhere Information Can Transform Lives', accessed September 2021.

New Zimbabwe (2021) 'High Court Orders Restoration of Internet Services, Zambia', *All Africa*, 15 August, accessed 17 October 2021.

Norman, D. (1988) *The Design of Everyday Things*, New York: Basic Books.

Nyamu-Musembi, C. (2005) 'Towards an Actor-Oriented Perspective on Human Rights', in N. Kabeer (ed.), *Inclusive Citizenship: Meanings and Expressions*, London: Zed Books, accessed August 2021.

Obia, V. A. (2020) '#EndSARS, A Unique Twittersphere and Social Media Regulation in Nigeria', *LSE Blog*, 11 November, accessed 17 October 2021.

OECD (2011) *OECD Guidelines for Multinational Enterprises*, Paris: OECD Publishing, accessed 17 October 2021.

OHCHR (1966) *Universal Declaration of Human Rights*, accessed 17 October 2021.

OHCHR (UN Office of the High Commissioner for Human Rights) (2011) *United Nations Guiding Principles on Business and Human Rights*, Geneva: United Nations, accessed 17 October 2021.

OHCHR (2015) *Joint Declaration on Freedom of Expression and Responses to Conflict Situations*, accessed 17 October 2021.

OHCHR (2019) 'Sudan: UN Experts Denounce Internet Shutdown, Call for Immediate Restoration', 8 July, accessed 17 October 2021.

Okunola, A. (2018) A Timeline of Internet Blockages in Africa, Tech Cabal. https://techcabal.com/2018/05/03/a-timeline-of-internet-blockages-in-africa/#:~:text=Guinea%20(February%202007),protests%20calling%20for%20his%20resignation.

Parker, B. (2021) 'Relief for Tigray Stalled as Ethiopian Government Curbs Access', *The New Humanitarian*, 11 February, accessed 17 October 2021.

Repucci, S. and A. Slipowitz (2021) *Democracy Under Siege*, Washington, DC: Freedom House, accessed 17 October 2021.

Reuters Staff (2018) 'UPDATE 2-Orange Official Calls Ivory Coast Telecoms Fire Act of "Sabotage"', *Reuters*, 15 May, accessed 24 August 2022.

Reuters Staff (2019) 'Some Internet Service Restored in Sudan After Court Ruling', *Reuters*, 9 July, accessed 17 October 2021.

Reuters Staff (2021) 'Sudan Court Orders Restoral of Internet, But No Sign of Services Returning', *Reuters*, 9 November, accessed October 2021.

Ritzen, Y. (2021) 'Rising Internet Shutdowns Aimed at Silencing Dissent', *Al-Jazeera*, accessed 26 October 2021.

Roberts, T. and A. Mohamed Ali (2021) 'Opening and Closing Online Civic Space in Africa: An Introduction to the Ten Digital Rights Landscape Reports', in T.

Roberts (ed.), *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*, Brighton: Institute of Development Studies, accessed September 2021.

Rozen, J. (2017) 'Journalists Under Duress: Internet Shutdowns in Africa Are Stifling Press Freedom', *Africa Portal*, 17 August, accessed 17 October 2021.

Shoker, S. and R. Shoker (2020) 'Using Artificial Intelligence to Predict Internet Shutdowns', accessed 17 October 2021.

Silas, D. (2021) 'Twitter Ban: ECOWAS Court Merges 4 Suits Against Nigerian Government', *Daily Post*, 9 July, accessed 17 October 2021.

Sruthijith, K. K. (2014) 'Firechat Was Sparking Interest in India, Even Before It Became a Mainstay of the Hong Kong Protests', *Quartz*, 1 October, accessed 17 October 2021.

Statista.com (2021) 'Number of Social Network Users in Nigeria from 2017 to 2026'.

Surfshark (2020) 'How to Do a VPN Speed Test and How to Read the Results', accessed 17 October 2021.

Tackett, C., N. Krapiva, and F. Anthonio (2020) 'As Conflict Escalates, Azerbaijan's Internet Shutdown Puts Lives Further at Risk', *Access Now*, 15 October, accessed 17 October 2021.

Taye, B. (2019) *Targeted, Cut Off, and Left in the Dark. The #KeepItOn Report on Internet Shutdowns in 2019*, accessed 17 October 2021.

Taye, B. (2021) 'Shattered Dreams and Lost Opportunities: A Year in the Fight to# KeepItOn', *Access Now*, accessed 17 October 2021.

The Star (2020) '*Al Shabaab Destroys Safaricom Mast in Mandera*', 18 December, accessed 24 August 2022.

Tiwary, D., A. Sharma, and N. Iqbal (2021) '18 Months After Split, Downgrade, 4G Mobile Internet Back in J&K', *The Indian Express*, 6 February, accessed 17 October 2021.

Tufekci, Z. (2017) *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, New Haven: Yale University Press.

UN Human Rights Committee (2011) *General Comment No. 34: Article 19: Freedoms of Opinion and Expression*, Geneva: United Nations, accessed August 2021.

UN General Assembly, Human Rights Council 2021 (2021) *Ending Internet Shutdowns: A Path Forward, Report of the Special Rapporteur on the Rights to Freedom of Peaceful Assembly and of Association*, Geneva: Human Rights Council, accessed 17 October 2021.

UNHRC (1999) 'General Comment 27, Freedom of Movement (Art.12)', *UN Human Rights Committee*, accessed 17 October 2021.

UNHRC (2012) *The Promotion, Protection and Enjoyment of Human Rights on the Internet A/HRC/32/L.20*, Geneva: United Nations Human Rights Council.

United Nations (1967) 'International Covenant on Civil and Political Rights', accessed October 2021.

United Nations Human Rights Council (UNHRC) (2016) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, New York: United Nations General Assembly.

Unwanted Witness (2021) 'News Brief: High Court in Uganda Sets Hearing Date for Internet Shutdown Lawsuit', *Unwanted Witness*, 30 March, accessed 17 October 2021.

Vertemati, L. (2021) 'Ethiopia's Internet Shutdowns: Contributing to Humanitarian Catastrophe in the Tigray', *Security Distillery*, 16 April, accessed 17 October 2021.

Woodhams, S. and C. O'Donnell (2021) 'The Tech Companies Behind Internet Shutdowns: Allot Ltd', *Top10VPN*, 29 June, accessed 17 October 2021.

Wyrzykowski, R. (2020) 'Mobile Connectivity in Sub-Saharan Africa: 4G and 3G Connections Overtake 2G for the First Time', GSMA website. https://www.gsma.com/mobilefordevelopment/blog/mobile-connectivity-in-sub-saharan-africa-4g-and-3g-connections-overtake-2g-for-the-first-time/.

Yural-Davis, N. and P. Werbner (eds) (1999) *Women, Citizenship and Difference*, London: Zed Books.