The Kill Switch

How Internet Shutdowns Threaten Fundamental Human Rights in Africa and Beyond

Felicia Anthonio

November 2022
## Contents

I. Introduction ................................................................................................................. 1  
II. The First Hurdle to Internet Access: Bad Policy that Prices Millions Out .......... 2  
III. The Second Hurdle: Legislation Blocking and Restricting Internet Access .......... 4  
IV. Internet Shutdowns: Growing Threats to the Exercise of Fundamental Rights in Africa, Worldwide .............................................................................................................. 6  
V. Internet Shutdowns: Activism in Africa and Around the World ......................... 8  
   Shutdowns Cannot Silence Citizens’ Voices During Protests, They Just Defer Them, An Illustration: ..... 8  
   The Early Days: Iran and Guinea .................................................................................. 9  
   Egypt: The Incident that Drew Global Attention to Internet Shutdowns ...................... 9  
   Cameroon: The Blackout that Shook Activism Against Internet Shutdowns in Africa .......... 10  
   Sudan: Internet Shutdowns to Quell Protests Against Military Coups ........................... 11  
   Nigeria: Twitter Bears the Brunt for Deleting President Buhari’s “Controversial” Tweet .......... 12  
VI. Internet Shutdowns During Elections Harm Democracies .................................. 13  
   Belarus: A Dark Day for Democracy in Eastern Europe .............................................. 13  
   Uganda: In the Dark During the Polls, Blocked in the Aftermath .................................. 14  
VII. Best Practices: Inoculating Societies Against Internet Shutdowns ....................... 15  
VIII. Recommendations for Policymakers and Other Stakeholders ............................ 17  
IX. Conclusion .............................................................................................................. 19  
Acknowledgements ....................................................................................................... 21
The Kill Switch: How Internet Shutdowns Threaten Fundamental Human Rights in Africa and Beyond

I. Introduction

The internet is an enabler of fundamental human rights, including the freedoms of opinion and expression, the freedoms of assembly and association, the right to the access of information, and the right to education. In 2018, the United Nations Human Rights Council reaffirmed its 2012 resolution on “the promotion, protection and enjoyment of human rights on the Internet.”¹ This resolution, adopted by consensus at the 38th Session of the HRC in Geneva, stated that “the same rights that people have offline must also be protected online . . . .”² But when the internet is purposefully disrupted or manipulated, so too are the rights of those using it. This infringement of rights can be seen clearly in the case of internet shutdowns. In 2016, nonprofit Access Now adopted the following oft-used definition of internet shutdowns during the launch of its global #KeepItOn campaign: “[a]n 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.”³ In simplified terms, “an internet shutdown happens when someone—usually a government—intentionally disrupts the internet or mobile apps . . . to control what people say online. . . . Shutdowns are also sometimes called ‘blackouts’ or ‘kill switches.’”⁴

People once relied upon traditional media outlets such as radio, print, or television to connect with the larger world. In many cases, these outlets were directly controlled by governments with an iron fist. The internet has empowered people to speak up, organize, and call out governments and policies that are detrimental to societal progress. Lived experience has shown that governments will often seek to curtail internet usage that contradicts their authority while simultaneously leveraging the internet to reach their citizenry through the widespread dissemination of government-approved information.
Today, the internet is essential for information distribution. During election periods, for example, politicians rely on the internet to inform their audience about their policies and plans through online campaigns. Citizens around the world have mobilized via digital spaces in order to protest unpopular governments, including in Egypt during the Arab Spring in 2011, in Sudan during the #IAmSudanRevolution in 2019 (which saw the ousting of former dictator Omar Al Bashir), and, more recently, in Nigeria during the #EndSARS protests against the brutalities committed by security forces against citizens.

In this paper, I explore the current state of free internet usage and potential threats to fundamental human rights in the digital age. In particular, I will focus on the introduction of restrictive and overreaching legislation and on internet shutdowns as methods of rights infringement. I will use various case studies from across Africa and apply key takeaways to the world at large. The African continent is the most diverse in terms of both the adoption of digital technologies as well as the representation of political ideologies. The region therefore serves as a microcosm for larger trends related to both internet usage and internet shutdowns that occur throughout the world. This paper concludes with recommendations for state and non-state actors to ensure open, accessible, secure, and fair internet for all, laying out a plan that will help to solidify the rights of billions in the digital world.

II. The First Hurdle to Internet Access: Bad Policy that Prices Millions Out

Even where citizens have access to the internet, authorities and service providers are finding new ways to lock out large swaths of the population from the digital world. Despite the significant role of the internet in advancing development and progress worldwide, there is still a major global digital divide—people across Africa are being priced out of access. While the global average internet penetration rate stood at over 66% as of December 2021, that of Africa stood at just 43%. Although internet connectivity and the use of electronic devices continue to grow across the continent, the high cost of data remains a barrier to widespread use, even for those who find themselves in spaces with sufficient connectivity. According to data provided by Cable UK, the cost of internet in Sub-Saharan Africa outpaces the rest of the world, with five Sub-Saharan nations among the top ten nations with the most expensive internet globally (including Botswana and Togo). This gap is
compounded by the fact that many communities with high data costs in Sub-Saharan Africa may also lack access to other basic needs including access to schools and hospitals, or even the basic necessities of food, water, electricity, and housing.

Given the indispensable role of the internet, there are a number of initiatives being piloted to bring more Africans online and close the digital gap. Initiatives like the SMART Africa project and the launch of the African Union’s Digital Transformation Strategy 2020–2030 by African Heads of State and Government aim to invest in the information, communications, and technology sectors to ensure affordable access to broadband connectivity and work toward sustainable and inclusive socioeconomic growth and development on the continent. African governments must continue to prioritize the fundamental rights of their citizenry through the implementation of these initiatives.

Even while pushing for increased internet connectivity with one hand, some African governments restrict access with the other by implementing measures such as access-limiting laws and digital tax policies.

Over the last five years, several governments in Africa, including those of Uganda and Ghana, have imposed or attempted to impose taxes or electronic duties on the use of digital applications and mobile money services. Kenya, Tanzania, and Sierra Leone have passed laws designed to police both online and offline spaces. The government of Uganda attempted to generate revenue through a daily “social media tax,” forcing consumers of social media to pay Ugandan Shillings (UGX) 200 (or US$0.05) per day to boost state coffers. Ugandan President Yoweri Museveni justified the policy as a “sin tax,” holding that it was necessary to punish social media users across the country for the consequences of their “opinions, prejudices [and] insults.” In 2021, the Ugandan government abandoned the social media tax in favor of a direct 12% levy on the net price of internet data, on top of which a value added tax of 18% will apply.

Ghana’s ruling government introduced an electronic transactions levy of 1.5% on electronic transfers and transactions on May 1, 2022. The government projects that imposing this levy will accrue about GHS6.9 billion (US$1.1 billion) in revenue annually for the government, which could help reduce the country’s budget deficit, revamp the economy, and build infrastructure. The Ghanaian opposition and a majority of Ghanaians, however, believe that adoption of this levy will be a blow on the country’s online businesses
and services as this additional burden will deter people from using electronic platforms. As access to the digital world in Ghana increases, many businesses are going online, relying on mobile money services to transact across the country and beyond. Although the imposition of the e-levy does not directly affect internet access, it will undoubtedly hinder internet accessibility, reducing the demographic that can afford to access key digital services and eventually slow down the development of e-commerce.

Bad policy has driven up the cost of internet access for millions of Africans over the last few years. This means that even where and when digital connectivity is available, people are being priced out of access to the digital world—and to their rights that come with that access. But price is not the only mechanism by which governments are restricting access: many governments have turned to legislation that restricts internet access more directly, as explored in the next Section.

III. The Second Hurdle: Legislation Blocking and Restricting Internet Access

Authorities across Africa have imposed regressive, exclusionary, and punitive laws focused on restricting free and fair access to the digital world. These policies are often justified by rhetoric that suggests that government control over the internet is necessary to prevent cyberterrorism, the spread of disinformation, or to crack down on unprotected classes of speech. The last few years have seen countries such as Kenya, Tanzania, and Sierra Leone introduce legal frameworks that police online spaces and curtail the freedoms of information and expression, and by extension, the freedom of association and freedom of the press.

Recent actions in Kenya highlight that new laws that move to curtail the freedom of expression online are being implemented. The Computer Misuse and Cybercrimes Act, signed into law in 2018, together with its amendments, create an environment that is unconducive to free expression and access to information by imposing harsh sanctions on internet users for vaguely defined offenses, such as “publish[ing] false, misleading or fictitious data or misinform[ation] with intent that the data shall be considered or acted upon as authentic” and “knowingly publish[ing] information that is false in print, broadcast, data or over a computer system, that is calculated or results in panic, chaos, or
violence among citizens of the Republic, or which is likely to discredit the reputation of a person.” The text of this law enables arbitrary and politically motivated enforcement by authorities. The law was promptly challenged in court, but despite this pending litigation, amendments to make the Act even more oppressive were introduced in Parliament in a move challenged by several members of civil society. The latest development in Kenya involves the introduction of an implementing authority, the National Cyber Command Centre, which has powers that would effectively limit the right to access information and the freedom of expression. Entrusting executive branch officials to issue internet access restricting regulations without effective statutory or judicial guardrails, coupled with the punishment of government critics, is a worrisome theme developing in the region.

Kenyan lawmakers have also mastered the art of hiding far-reaching, rights-suppressing amendments in complex omnibus laws. In 2021, Kenyan lawmakers introduced amendments to the Official Secrets Act (Cap 187) that effectively handed discretionary powers to the Cabinet Secretary Interior and Coordination of National Security to access data from any phone or computer. The same amendment introduces harsh sanctions for noncompliance: time in jail, monetary fines up to KSh1,000,000 (~ US$8,795), or both. Laws such as this are a great affront to the right to privacy. They can also have chilling effects over speech criticizing officials.

Tanzania is not far behind in the implementation of draconian laws that limit fundamental rights, including free expression, the right to privacy, and the right to access information. Tanzania has in the past few years passed a number of laws including the Electronic and Postal Communications (Online Content) Regulations (2020), Media Services Act (2016), and the Cybercrimes Act (2015). These laws introduce, among other things, the criminalization of defamation and the introduction of government-controlled licensing of newspapers and online spaces. The Online Content Regulations, which were passed just months before the country’s general elections in 2020, also prohibit the use of or distribution of circumvention tools, such as virtual private networks (VPNs), that allow access to prohibited content. This move is dangerous and limits the capacity of people to anonymously and freely use the internet online. This shift away from free internet use set the stage for future restrictions: it was thus unsurprising that authorities in Tanzania imposed internet shutdowns during the 2020 elections.
In Sierra Leone, a similar story played out. Although the government decriminalized libel and sedition, it also introduced a cybercrimes bill in 2021 that sought to introduce arbitrary, non-adversarial legal processes, and established overbroad classes of offenses without defining clear penalties or implementation guidelines, instead leaving it up to the relevant minister to unilaterally implement follow-on policy to clarify the law. Once again, this action affirmed and expanded the executive’s power and control over online spaces.

It is of note that most of the countries introducing these laws are signatories to international and regional legal instruments that guarantee the very rights they seek to unreasonably limit. Both Tanzania and Kenya are, for example, signatories to the International Covenant on Civil and Political Rights (ICCPR), which guarantees the right to privacy in Article 17, the freedom of expression, and the right to access information in Article 19. They are also signatories to the African Charter on Human and Peoples’ Rights (ACHPR), which guarantees the freedom of expression and right to access information in Article 9. Yet these international frameworks are doing little to prevent the rollback of the rights of citizens in the digital world across the continent.

IV. Internet Shutdowns: Growing Threats to the Exercise of Fundamental Rights in Africa, Worldwide

As the true potential of the internet and digital communication platforms as a space for organization, mobilization, information exchange, and expression takes root, authoritarian regimes all over the world have seized every opportunity to curtail and control the growth of online spaces. This is clearly exemplified by the widespread use of internet shutdowns by governments in times of civil strife. Between 2016 and 2021, Access Now’s Shutdown Tracker Optimization Project (STOP) documented at least 925 incidents of shutdowns across the globe in 73 countries, including India, Kazakhstan, Tajikistan, Myanmar, Cuba, Iran, Belarus, Yemen, Afghanistan, Ethiopia, the Democratic Republic of Congo, Sudan, Algeria, Burkina Faso, Uganda, Burundi, Tanzania, Guinea, Togo, and Cameroon. Within this period, India has been the most frequent perpetrator of internet shutdowns worldwide. In 2021, Access Now and the #KeepItOn coalition documented at least 106 incidents of shutdowns in India, a majority of which happened in Jammu and Kashmir. Myanmar followed suit with at least 14 incidents of shutdowns, while Sudan and Iran...
recorded five and four incidents, respectively. Fourteen countries in Africa disrupted internet access 25 times, two more countries than the previous year. Importantly, five new countries—Burkina Faso, Eswatini, Niger, Senegal and Zambia—shut down the internet for the first time in 2021, in what is a very foreboding trend for Africa.

Most shutdowns occurred during key national moments, including elections, protests, conflict, or communal violence. Some governments repeated the process several times over a single period of strife. Chad, the Republic of the Congo, Uganda, and Zambia flipped the switch during elections in 2021, and shutdowns were imposed in response to protests and civil unrest in Eswatini, Ethiopia, Gabon, Senegal, and South Sudan. Ethiopia remains the biggest perpetrator in Africa, with at least 23 recorded shutdowns since 2016. Ethiopia’s Tigray region is also currently experiencing the longest complete internet blackout in Africa, which began in November 2020.21

In most instances, government-ordered internet shutdowns are “complete” or “blanket” shutdowns, which block all access to the internet across a given region. Governments have also slowed down internet speeds in what is known as “throttling,” or blocked specific digital platforms. Internet shutdowns can be referred to as “blackouts,” “hitting the kill switches,” or “network disruptions.” Access Now’s STOP documents and verifies shutdowns as they happen globally and provides a repository of up-to-date data on internet shutdowns globally. Frighteningly, governments are becoming increasingly sophisticated in imposing shutdowns and blocking communications, using tactics such as fundamental infrastructure shutdown, deep packet inspection (DPI), and filtering, among others.22 It is essential to understand the different ways that the internet can be shut down to better understand, prepare for, circumvent, and document shutdowns.

Internet shutdowns have increasingly become a part of government playbooks in Africa and around the globe, in democratic and authoritarian regimes alike. Authorities tend to impose internet shutdowns during high tension moments, including elections, protests, conflicts, and coup d’états. Governments justify the use of internet shutdowns during these key national events by citing the need to restore public safety and order, to prevent the spread of disinformation or hateful content, or to lessen incitement to discrimination, hostility, and violence;23 to prevent cheating during exams;24 or to fight banditry.25 On some occasions, no explanation is given by authorities for the shutdowns imposed.
For instance, the government of Uganda ordered ISPs in the country to completely shut down the internet on the eve of the election in January 2021, citing national security. Countries in the Middle East and North Africa, such as Algeria, Iraq, Sudan, and Syria, tend to shut down the internet to quell protests or “prevent cheating” during school exams. In 2021, authorities in Nigeria’s Zamfara and Katsina states imposed shutdowns to disrupt the activities of criminal groups in a move which most people saw as counterproductive. Last year, the governments of Nigeria and Uganda blocked access to Twitter and Facebook, respectively, in retaliation for the companies’ removal of government-sponsored content which violated the platforms’ community standards. Twitter was unblocked in Nigeria after seven months, while in Uganda Facebook remains inaccessible without the use virtual private networks. Although governments try to justify internet shutdowns with gestures toward national security, these acts of repression and censorship contravene human rights law which requires that any limits to public freedoms and rights must be necessary, proportionate and nondiscriminatory. Internet shutdowns fail to meet these requirements, thereby violating the people’s rights to freedom of expression, peaceful assembly, and association enshrined under Articles 19, 21, and 22 of the International Covenant on Civil and Political Rights (ICCPR).

V. Internet Shutdowns: Activism in Africa and Around the World

Shutdowns Cannot Silence Citizens’ Voices During Protests, They Just Defer Them. An Illustration:

In recent years, there has been an increase in the use of internet shutdowns and excessive force by governments against protesters as a measure to control protests and demonstrations, both across the African continent and worldwide. The use of these repressive measures often results in the violation of the fundamental rights of citizens, such as freedom of expression, access to information, assembly, and right to life. While people power finds a way, blocking internet access makes it more difficult for people to make their voices heard.

As the role of the internet continues to expand in the everyday life of citizens, so too grows the impact of internet shutdowns. Although shutdowns tend to be ineffective in silencing
citizens, as protests continue to gather momentum despite the closing of digital space, shutdowns disrupt people’s ability to coordinate and organize efficiently. The case studies below shed more light on how citizens and civil society in Africa and around the world have resisted government-mandated internet shutdowns through advocacy, mobilizations, litigation, and solidarity.

The Early Days: Iran and Guinea

Iran and Guinea were some of the earliest nations to carry out internet shutdowns during a period of civil unrest. In 2009, Iranian authorities throttled internet speed in response to protests against the disputed outcome of that year’s presidential elections. Similarly, in 2007, Guinea was the first known country to have ordered a full-scale internet blackout, impacting more than a quarter of the nation’s online population. The shutdown was ordered by then President Lansana Conte under a decree of martial law following widespread protests demanding his resignation.

Egypt: The Incident that Drew Global Attention to Internet Shutdowns

Internet shutdowns started to gain popularity among authoritarian governments in 2011 during the Arab Spring. Authorities in Egypt cracked down on the internet and digital platforms in an attempt to quell protests against longtime Egyptian President Hosni Mubarak in Tahrir Square, serving as a model for subsequent government action across the globe. As protests erupted on January 25, 2011, the government began by instituting blocks on Twitter and Facebook and eventually shut down internet access across the entire country by January 28. This was a deliberate attempt by the authorities to prevent the people of Egypt, who relied heavily on these platforms, from mobilizing and coordinating their demands during the protests. Nonetheless, the youth in Egypt remained steadfast in making their demands clear, as what began as online protests turned into mass street protests resulting in the resignation of President Hosni Mubarak. The scale, scope, and impact of the shutdown in Egypt took digital civil rights experts by surprise. The events around this uprising prompted a team of computer scientists at the internet monitoring firm Renesys to begin to document and report about the internet shutdown in Egypt. At the same time, digital rights advocacy organizations were making efforts to assist and provide support to Egyptian activists to circumvent surveillance and blockages of internet communications and services.
Cameroon: The Blackout that Shook Activism Against Internet Shutdowns in Africa

Beginning in 2017, the Cameroonian government shut down the internet for at least 230 days in an attempt to tamp down on the free speech and civil rights of activists of the minority Anglophone Cameroonian community. Activists in English-speaking regions of Cameroon were protesting against systemic political, linguistic, and economic discrimination. The first part of the shutdown, lasting 93 days, was a complete internet blackout. A second shutdown targeted social media platforms. The government justified the shutdown by appealing to national security, but the reality on the ground showed that the internet shutdowns escalated the crises and left people in a heightened state of confusion and fear.

Cameroon’s internet shutdown serves as a classic example of how governments are able to control freedom of expression and other fundamental rights during a national crisis. It further highlights the use of shutdowns by long-serving regimes, as well as the harm and counterproductive nature of this practice to silence people’s voices against unpopular government policies. The shutdown was an excuse by the government to cripple the biggest civic uprising in Cameroon’s history.

The shutdown forced Anglophone Cameroonians to drive to the French-speaking parts of the country to be able to access the internet, potentially endangering their lives in the process. This further highlights the weaponization of shutdowns by governments; Anglophone Cameroonians had to endure blatant violations of their human rights and freedoms in retaliation for standing up against injustice and discrimination by Paul Biya, Africa’s second-longest serving president. The internet blackout has left an imprint on Cameroon’s sprouting internet ecosystem by forcing young and promising technologists, innovators, coders and entrepreneurs to flee Buea, also known as “Silicon Mountain”—once heralded as Africa’s next tech hub. To date these young people, some of whom had an opportunity to travel to developed countries, have not returned, depriving Cameroon’s English-speaking region and the country as a whole of these young talents.

The people of Anglophone Southwest and Northwest Cameroon have, however, remained determined to have their voices heard and are supported with overwhelming solidarity by the international community. The shutdown in Cameroon was a wake-up call for activists in civil society who had committed under the #KeepItOn campaign in 2016 to fight internet
shutdowns globally. Several organizations, including Internet Sans Frontières, Access Now, Open Observatory of Network Interference (OONI), the African Freedom of Expression Exchange (AFEX), who are members of the global #KeepItOn coalition, joined Cameroonianists both locally and in the diaspora to raise awareness about the shutdown and the atrocities that accompanied it in the widespread #BringBackOurInternet online campaign. That became one of the most widely used hashtags, attracting even tweets from high-profile figures such as Edward Snowden, to advocate both locally and internationally against internet shutdowns.

**Sudan: Internet Shutdowns to Quell Protests Against Military Coups**

Authorities in Sudan have shut down the internet and social media platforms often to quell protests. On December 19, 2018, authorities began shutting down social media platforms including Facebook, Twitter, WhatsApp, and Instagram amid protests surrounding the rising cost of living and the fast-dwindling economy of the country. Security agents in Sudan, in response to massive protests, fired live bullets and tear gas at protesters. This resulted in the killing of about 20 persons, and several were injured while numerous opposition leaders were arbitrarily arrested for taking part in the protests. The civil disruption lasted until February 26, 2019. The months-long mass protests intensified and eventually led to the ousting of former dictator Omar Al-Bashir by the Sudanese army on April 11, 2019. Following the fall of the Al-Bashir government, the Sudanese people demanded a return to civilian rule. In a calculated and preemptive manner, the Transitional Military Council (TMC) on June 3, 2019, shut down the internet for over a month and blocked the access of foreign media before embarking on a brutal crackdown on protesters, resulting in the coordinated killing of more than 100 people, the injuring of over 700, and the rape of at least 70. With a shutdown of this nature in place, authorities guaranteed that the rest of the world would be kept in the dark. Internet shutdowns empower authorities to perpetrate crimes and serious human rights violations against people with impunity.

Two years later, on October 25, 2021, the Sudanese military overthrew the transitional government and arrested several officials, including the prime minister. As the Sudanese people denounced the military coup in mass protests, the authorities ordered internet service providers to shut down the internet, affecting both mobile and fixed cable connections throughout the country for 25 days. According to reports, at least 17 people
were killed and over 250 injured during this shutdown. In both 2019 and 2021, internet access was restored for all internet users in Sudan after citizens challenged the blackouts in court.

**Nigeria: Twitter Bears the Brunt for Deleting President Buhari’s “Controversial” Tweet**

In June 2021, Authorities in Nigeria shut down access to Twitter for over seven months citing “persistent use of the platform for activities that are capable of undermining Nigeria’s corporate existence.” However, the timing of the ban makes the government’s justification questionable: the ban came immediately after Twitter’s decision to delete a tweet by President Muhammadu Buhari that incited violence against Nigerian citizens from the south among a wave of online oppression during the #EndSARS protests.

The Twitter ban came along with threats from government officials that anyone found to be using Twitter within the country would face harsh sanctions despite a dubious legal foundation for this claim. Many in Nigeria defiantly continued to tweet using VPNs. They joined the international community in condemning the Nigerian government for this shutdown. As the use of VPNs skyrocketed, the government issued a statement threatening to arrest and charge anyone who continued to use the social media platform. Notably, the Nigerian Communications Commission, which was asked to collaborate with prosecutors to ensure “speedy prosecution of offenders without any further delay,” distanced themselves from this shutdown, stating that it was not within their jurisdiction to take part in such prosecutions.

The government eventually restored Twitter access to the country, more than half a year after the directive was issued, claiming that Twitter had agreed to adhere to several conditions set by the government as a precursor to their resumption of operations. Neither party, as at the time of writing this paper, has made public the content of these specifications, leaving stakeholders apprehensive over how this could affect the freedom of expression, right to association and right to access information among other human rights in the long run. In a landmark ruling, the Community Court of Justice of the Economic Community of West African States (ECOWAS Court) on July 14, 2022, declared the seven-month Twitter blocking in Nigeria unlawful and incongruent to the African Charter on Human and Peoples’ Rights as well as the UN Charter. The court also ordered the Nigerian government to take appropriate legislative steps to guarantee plaintiffs’ rights and
to pay litigation fees.\textsuperscript{45} At the time of writing, full implementation of the decision by the Nigerian government is still underway.

VI. Internet Shutdowns During Elections Harm Democracies

Internet shutdowns do not happen in isolation. Governments often switch off the internet at a time when the digital world serves as a critical lifeline to people and communities in crisis or tumult. For example, internet shutdowns often occur during close or contested elections. Elections, especially in growing democracies, are a critical time of transition, and active citizen participation in the electoral process contributes significantly to credible democratic outcomes. When a shutdown is implemented during an election, democracy itself is attacked, and international observers cannot scrutinize and safeguard election outcomes. This provides leeway for governments to manipulate election outcomes. Internet shutdowns thus mar the credibility of election results, and citizens may question the validity of the election as a whole. In a majority of countries where internet shutdowns occur during elections, the incumbent gained control and stayed in power, as seen in Uganda, the Republic of Congo, and Guinea. Governments who want to hold on to power are likely to impose shutdowns at times that favor them most, according to a study by the Collaboration on International ICT Policy on East and Southern Africa (CIPESA).\textsuperscript{46}

Belarus: A Dark Day for Democracy in Eastern Europe

It is important to note that internet shutdowns are not limited to Africa. Although this paper has focused on the African context, there is a long and unfortunate history of government-sponsored internet shutdowns beyond Africa. For example, on election day in 2020 in Belarus, as feared by much of the international community, reports of partial internet shutdowns affecting social media platforms began to emerge.\textsuperscript{47} Landline and mobile services within and outside of the country were also inaccessible. That same day, in the middle of the blackout, Belarusian electoral officials declared victory for incumbent President Aleksandr Lukashenko.\textsuperscript{48} The people of Belarus challenged the election outcome in massive protests, to which the government responded with a complete internet blackout. Security forces attacked protesters with water cannons, stun grenades, and rubber bullets in order to disperse them.\textsuperscript{49} The Belarusian people were digitally cut off from the rest of the world for questioning the credibility of the election’s outcome, preventing them from communicating with families, friends, and the outside world.
Uganda: In the Dark During the Polls, Blocked in the Aftermath

In the run up to the heavily contested 2021 general elections, the government of Uganda ordered a countrywide internet shutdown, citing national security concerns. In a live broadcast in which President Museveni announced the internet shutdown order, he accused Facebook of meddling in the country’s national affairs after the platform took down content of government officials. By the time the country went to the polls, many citizens were in the dark, unable to access impartial news sources and unable to voice their concerns. This is a clear illustration of the way in which internet shutdowns lead to violations of human rights, especially the right to access to information and the freedom of expression. Museveni’s government proceeded to lift the ban after he was declared the winner, five days after it first began. But even then, several social media sites including Facebook, Twitter, and YouTube remained blocked for a few more days. International and local human rights groups condemned the internet and social media blackout.

This was not the first time that the Ugandan government had employed the use of internet shutdowns in an attempt to control the flow of information and stop dissent in its tracks. The government also shut down social media platforms on election day in 2016, again citing national security concerns. The veracity of these claims remains unestablished, and the president’s word should not be taken as truth, especially when these shutdowns are so often used for the benefit of his office and the security of his term. In 2016, in addition to the social media blackout, the government also suspended mobile money transfers, a service relied on by a large part of the population. This left many people without access to their money and, therefore, without access to necessary sustenance. Users of mobile money transfer services cited inability to pay for basic needs including food, water, and electricity, and some guardians could not pay school fees for their children in the days following the suspension of services.

Shutting down the internet during elections often leaves people with more questions than answers. As noted, it mars the credibility of the outcome of elections and disrupts the democratic process. It is a widely posited theory, that the 2016 and 2021 elections were not conducted freely and fairly. In 2021, the East African Law Society filed a yet-to-be-heard suit against the government of Uganda, challenging its decision to shut down the internet during both general elections.
VII. Best Practices: Inoculating Societies Against Internet Shutdowns

Internet shutdowns are a growing threat. Over the past several years, they have crept across Africa and across the globe. This rapid proliferation has shown that shutdowns move across borders, infecting more and more societies with these novel restrictions on fundamental rights. In light of this, ensuring that people around the world are able to enjoy free and open internet access—especially as political instability rises—requires preventative action. Important steps to that end include raising the social and political costs of enacting internet shutdowns by creating normative frameworks to ensure that shutdowns are never imposed without strict adherence to international human rights law.

Raising these social and political costs can be achieved by democratic governments themselves, through clear commitments to a free and open internet. Ghana and Kenya are among the list of countries in Africa that have not imposed internet shutdowns, while Benin, Liberia, and Senegal are one-time offenders. Recently, Ghana’s Minister for Communication and digitalization, Ursula Owusu, during the launch of the Danish Tech for Democracy Pledge initiative, reiterated the government’s commitment never to shut down the internet in the country (although she made clear that the government would take the spread of misinformation seriously). In 2020, Ghana’s communications regulator, the National Communications Authority (NCA) pledged to keep the internet and digital communications tools accessible and open throughout the election period following fears expressed by the opposition ahead of elections. This commitment builds off of a similar commitment made in 2016 by then President of Ghana John Dramani Mahma, who publicly assured Ghanaians that his administration would not disrupt the internet during elections as intimated by the Inspector General of Police (IGP) at the time. Civil-society actors and other stakeholders played a crucial role in holding the Ghanaian authorities accountable in both instances.

Unlike Ghana, Benin shut down the internet and social media platforms for at least 24 hours in 2019, coinciding with legislative elections. However, in a positive turn of events, the Beninese authorities did not cut internet access during the country’s presidential elections in April 2021. Prior to the elections, the #KeepItOn coalition in an open letter appealed to the government not to disrupt internet access. The tendency of a government
to repeat an internet shutdown is very high, but pressure from outside organizations and the local citizenry can push against rights-suppressing shutdowns.

Kenya also remains committed to keeping the internet on during important events in East Africa, although the same is not true of her neighbors, Uganda and Tanzania. On two occasions, the Interior Cabinet Secretary of Kenya, Fred Matiang’i, indicated the government would not shut down the internet as the country went to the polls in August 2022. However, as in the rhetoric employed by Minister Owusu in Ghana, he indicated the Kenyan government was going to take the spread of misinformation and hate speech seriously. In the midst of the election period, the National Cohesion and Integration Commission (NCIC) threatened that authorities would shut down Facebook if Meta (its parent company) did not take appropriate measures to curtail the spread of hateful content on its platform. This comment was condemned by several civil-society organizations as well as government officials. Consequently, representatives of the government reassured the people of Kenya that the internet and digital platforms would not be shut down. While civil society and other relevant actors remain hopeful that more countries in the region will look up to Ghana and Kenya, among others, in order to preserve digital rights across Africa, it is important to underscore that authorities in both countries are committed to upholding the fundamental rights of their citizenry by ensuring unfettered access to the internet during critical times in the countries.

Legislation can also be an instrument in inoculating societies against shutdowns. An example here is the Preventing Unwarranted Communications Shutdowns Act, a bill introduced in the U.S. House of Representatives in October 2020 by Representatives Anna Eshoo and Morgan Griffith. This bill seeks to limit presidential powers to control or shut down communications networks, including the internet. At present, the Communications Act gives the president the power to take control of communications facilities or equipment in certain circumstances. If this power is left undefined, it could result in shutdown orders being easily available to the holder of the office. Eshoo and Griffith’s bill sets in place solid structures and due process within which a sitting president may operate should there be a need to shut down the internet. This includes a checks and balances system whereby the president is required to notify Congress either before or not more than 12 hours after making such orders and gaining approval from at least three-fifths of the House and Senate.
In addition to the checks and balances system, the bill introduces accountability mechanisms aimed at safeguarding against the misuse of the national security justification in the implementation of shutdowns. The president, in order to issue a directive for the internet to be shut down, would have to issue a notification of what “imminent threat” necessitated the shutdown, a description of the shutdown order—which would include, among other things, the geographical scope and the types of communications networks that would be affected by the order—as well as the time within which the order would persist.

This bill is a good example of actions that could be taken by States to ensure the protection of human rights and to prevent the arbitrary application of executive power, as is often the case in countries that implement shutdowns. It is essential for other countries around the globe to adopt similar policies, which make it extremely difficult for one actor to authorize internet shutdown orders.

**VIII. Recommendations for Policymakers and Other Stakeholders**

Governments, private companies, academia, civil-society organizations, the media, and private individuals must join forces to fight internet shutdowns. All stakeholders have a part to play to ensure that access to the global internet landscape remains widespread in Africa and beyond.

Legislatures can lead the charge in the fight to preserve access to a free, secure, and open digital space. The struggle for an open internet requires that lawmakers promote laws that align with constitutionally-founded principles of access, equity, and democracy. Laws that disproportionately limit human rights should not be the standard. Moreover, bills such as the Preventing Unwarranted Communications Shutdowns Act in the United States should be enacted even when the threat of a shutdown is not imminent, in order to hold executives to account and increase public confidence that governments will not have the power to arbitrarily shut down the internet.

But the duty to preserve the fundamental rights of the citizenry does not stop with the legislature. Executives, too, have a part to play. Governments must recognize their constitutional responsibilities to protect the fundamental rights of their citizenries and
refrain from shutting down the internet even during crises. Executives that fail to uphold these rights by ordering arbitrary or politically motivated shutdowns should incur retributive or deterrent penalties. On the other hand, those executives that do not participate in internet shutdowns must collaborate and remain in dialogue with those who do to persuade them to not impose shutdowns.

Borrowing a leaf from the ECOWAS and Sudan courts, international, regional, and national courts should step up to the plate and make themselves heard on matters of internet shutdowns. Drawing from the example of the ECOWAS court, challenges as to jurisdiction were adequately addressed and thrown out, creating jurisprudence that will ensure regional courts can adjudicate local matters. The courts in Sudan illustrated as well that there are other avenues through which human rights can be considered, such as consumer protection laws. Throughout these processes, courts have regularly engaged stakeholders and experts to better understand internet shutdowns and their effect.

Regional and international bodies such as the United Nations, European Union, and African Union must introduce binding resolutions that contemplate repercussions for governments who shut down the internet. They also should continue to highlight the threats of internet shutdowns on the enjoyment of human rights, through efforts like the recently published report by the Office of the UN High Commissioner for Human Rights (OHCHR).59

Private actors also have key roles to play in the multi-pronged fight against internet shutdowns. First, internet service providers and social media platforms must be transparent about government requests for information about customers or users to ensure that they are not complicit in a rights-suppressing regime. Open communication with the public and the news media about persistent or threatening government action will make it more difficult for governments to covertly implement targeted directives contrary to human, civic, or social rights. In cases where government requests violate national or international norms regarding privacy, free speech, or political protest, the companies should leverage their power by delaying compliance and potentially challenging the requests in court.

Additionally, civil society organizations can empower citizens by providing civic education on human rights and the impact of internet shutdowns: the best protection against human rights violations is the knowledge of and assertion of one’s individual rights. People who
know what is owed to them by law are more likely to resist attempts to suppress their rights. These organizations and campaigns, like #KeepItOn, can continue to name and shame authorities responsible for internet shutdowns, creating awareness around these actions as a deterrent to future shutdowns.

Public and private actors alike have key roles to play to fight back against a worrying spate of rights-suppressing internet shutdowns that have been occurring in Africa and beyond. Together—through combined efforts to change the law, enforce new political norms, push back against authoritarian government tactics, further education, and assert individual rights—stakeholders can fight for a future with open, unfettered access to the resources available in a digitally-connected world.

**IX. Conclusion**

Internet blackouts violate fundamental rights of people across the globe. Worse, they often provide cover for state and non-state actors to perpetrate human rights abuses with impunity. Shutting down the internet during crises, conflicts, and strife results in denying people the ability to communicate with their families and friends, amplifies the spread of false information and rumors, and severely curtails freedom of expression, assembly, and speech. Shutdowns during elections devalue democracy, denying citizens the ability to actively participate in their election and destroying trust in the election’s result.

Nations have lost billions of dollars to internet shutdowns, yet the practice remains common. For instance, a study by the Organization for Economic Co-operation and Development (OECD) estimated the economic loss caused by the 2011 internet and communication blackout that happened in Egypt was at least US$90 million. It is important to note that this amount excludes the secondary economic impacts which resulted from a loss of revenue in other sectors such as e-commerce, tourism, and call centers. Top10VPN reported that the global economy has lost a whopping US$35.5 billion since 2019 as a result of government-mandated internet shutdowns. Such a drain on the world’s finances is unacceptable, especially as large swaths of the global population may struggle with basic daily needs.
Despite the glaring negative impact of shutdowns on human rights and lives, and the availability of regional and international frameworks denouncing their use, governments continue to employ them around the world. The internet is an integral ingredient that equips people with skills and information to realize their dreams. It is therefore important for stakeholders around the world to unite forces in order to combat internet shutdowns globally.
Acknowledgements

The author would like to thank Bridget Andere and Alexia Skok for their immense contributions to this paper. She would also like to thank Artur Pericles Lima Monteiro and Sachin Holdheim for their input and review of the paper.
References

2 Id.
7 See Who We Are: The Beginning of a New Era, SMART AFRICA, https://smartafrica.org/who-we-are/.
9 Id.
15 Id.
17 Id.
26 Anthonio & Díaz Hernández, supra note 24.
27 BREAKING: Sokoto States Shuts Down Telecommunication Networks After Zamfara, Katsina, supra note 25.
33 Id.


About the Author

Felicia Anthonio is #KeepItOn Campaign Manager at Access Now. Anthonio leads the campaign’s global advocacy efforts by raising awareness, monitoring and documenting the devastating impact of shutdowns on people’s lives, and engaging with policymakers to end internet shutdowns.

She holds an M.A. in Lettres, Langues et Affaires Internationales and a B.A in French and Psychology from l’Université d’Orléans, France, and the University of Ghana, respectively.

Digital Future Whitepaper Series

The Digital Future Whitepaper Series, launched in 2020, is a venue for leading global thinkers to question the impact of digital technologies on law and society. The series aims to provide academics, researchers, and practitioners a forum to describe new challenges of data and regulation, to confront core assumptions about law and technology, and to propose new ways to align legal and ethical frameworks to the problems of the digital world.

The Digital Future Whitepaper Series is led by ISP visiting fellow Andrew Burt and co-edited by ISP Wikimedia fellow Artur Pericles Lima Monteiro and ISP affiliate fellow Nikolas Guggenberger. Sachin Holdheim (Yale Law School ’24) served as the research assistant for this whitepaper.

Information Society Project

The Information Society Project (ISP) is an intellectual center at Yale Law School, founded in 1997 by Professor Jack Balkin. Over the past twenty years, the ISP has grown from a handful of people gathering to discuss internet governance into an international community working to illuminate the complex relationships between law, technology, and society.