# TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

3 INTRODUCTION

6 VARYING MODES OF INTERNET SHUTDOWNS

9 THE IMPACT OF INTERNET SHUTDOWNS

   Economic Impact
   Socio-Political Impact

14 THE ROOTS OF INTERNET SHUTDOWNS

   Justifications
   Motivations & Power Relations
   The Power of the Courts
   The Power of the Private Sector
   The Power of Traditional Media & the Public
   Non-Governmental Causes

22 NORMATIVE CONSIDERATIONS

24 CONCLUSION

26 REFERENCES

30 APPENDIX
Internet shutdowns – where access to the internet is cut off within a country’s borders – are not a new phenomenon; it is the increasing scope and scale that make this an urgent issue. In India, there were more than 130 separate instances of government-ordered internet shutdowns in 2018; while the African continent holds the record for the longest shutdowns, with countries like Cameroon and Chad as particularly notable cases. Choosing to shut off access to the internet is choosing a particularly blunt instrument, one that appeals to certain governments, but also one that is unlikely to persist or remain unchanged as governments increase their surveillance capacity and improve their more targeted tools for co-opting and manipulating public opinion.

Given the urgency of this issue in the African context, a workshop on internet shutdowns was jointly convened by the University of Oxford’s Programme in Comparative Media Law & Policy at the Centre for Socio-Legal Studies and the University of Johannesburg’s School of Communication in 2018 in Johannesburg. It hosted two dozen participants across the continent representing a wide array of academic disciplines and practitioner fields, including from law, communications, and computer science disciplines, and from the legal, advocacy, and technology sectors. Countries discussed included: Burundi, Cameroon, Ethiopia, Kenya, Morocco, South Sudan, Uganda, and Zimbabwe.

Overall, during the workshop, despite the rising instances of internet shutdowns in Africa, the urgent need for more research became apparent, particularly research that looks in-depth at the social, political, economic, and legal contexts in which internet blockages are embedded and the very different types of shutdowns that occur. The work of advocacy organizations serves a function in increasing public awareness, but the debate on this complex issue requires more nuance and time-consuming research than many advocacy organizations have the resources to do. As a result, this report is intended to help provide a basis for guiding future work; it offers both insights on the discussions that took place during the two-day workshop and a review of the important research that does exist. In addition, below we offer a few key suggestions that emerged from the workshop about the direction we believe research needs to go. Such research could not only help advocacy organizations, but also policymakers grappling with building regulatory frameworks to keep up with the rapid technological advancements happening around the world.

Internet shutdowns should be treated as a spectrum rather an on/off switch

Internet shutdowns should not be treated as homogeneous. Rather, they exist on a spectrum – varying along dimensions such as duration, breadth, depth, speed, and frequency. Treating them as such allows that discussion to stay engaged with changing debates about the evolving, and competing, norms governing the internet.
Impact of shutdowns: More attention to the less visible impacts of shutdowns is needed

There are a number of studies that focus on the economic impact of shutdowns. Yet, while the economic argument may work for governments with a higher internet penetration rate, it may be less effective for others, particularly when concerns about national security, violent conflict, or terrorism are at the forefront (and have their own economic impact). More research is needed that looks at the other dimensions of impact, including, for example, the impact on those in the poorest communities who lack access to the internet to begin with.

Root of shutdowns: More attention to the role of non-governmental actors is needed

In popular debates about the causes of internet shutdowns, governments are almost always seen as the perpetrators. Yet existing research and the debate at the workshop show how varied the causes can be – from the unintentional, including severe weather and accidentally severed cables, to the intentional but non-governmental, such as foreign government attacks, rogue hackers, or ISP led slowdowns. Even where governments are the causes, more attention needs to be payed to the role of other actors to help understand why governments make the choices they do. The role and power of a range of different stakeholders should be considered, from the courts to mainstream journalists, sitting government officials to political candidates, domestic publics to foreign publics, and local ISPs to international social media companies, to the likes of even terrorist organizations and the military. Focusing on the kinds of power relations that exist and how power is exerted between them could provide productive insights into opaque government decision-making processes.

Normative issues: A broader debate about the balance between protecting human rights online and protecting security is needed

Despite vocal condemnations of internet shutdowns, particularly from human rights organizations, the acceptability of some forms of internet restriction appears to be on the rise. Following the violent attack in Sri Lanka, a handful of those who had long advocated for a free and open internet wrote approvingly in outlets like the New York Times and the Guardian about the government’s decision to restrict access during the attack in the hopes of minimizing the spread of misinformation. With scandals like Cambridge Analytica and Facebook’s role in perpetuating the Rohingya genocide, the era of seeing social media’s impact on the world as necessarily positive has long passed. Given such changes, we believe a broadened debate about internet shutdowns is greatly needed. One that takes us away from the previous polarization pitting civil society and human rights advocates and social media companies on the one side against governments on the other, and instead towards a debate that takes into account the very real challenges many states face about how to protect the safety of their citizens at the same time as protecting human rights.
Internet shutdowns are not a new phenomenon; it is the increasing scope and scale that make this an urgent issue. Debates over whether there should be a ‘kill switch’ for the internet, particularly in the context of cyberwarfare, have emerged in a range of jurisdictions (including the US, UK, and Turkey). While much has been written about the censorship strategies of authoritarian governments, less focus has been given to the choices some make to shut off access to the internet. It is the totality, the bluntness, and the intentionality of shutdowns that stand them apart from more targeted efforts at censorship, whether blocking certain websites, arresting particular bloggers, or making it a crime to post messages about an unfolding event on social media.

The current one is likely a unique moment in the life of internet shutdowns. They are a tool that appeals to certain governments but also one that is unlikely to persist or remain as popular as governments increase their surveillance capacity and improve their more targeted tools for co-opting and manipulating public opinion. More subtle tactics are gaining traction such as the unleashing of troll armies on critics that can involve many people adopting fake identities and flooding social media or particular forums with a specific message and the intention to drown out opposing voices. Bots, or automated programmes, have also been effective at distorting conversations by overwhelming certain platforms with misinformation and fake news. The growing concern is, as some have argued, not censorship or the restriction of voices but actually too much information, much of it low quality and even harmful, and the competition inherent in the modern attention economy. Governments are increasingly finding innovative ways of discouraging the use of certain social media platforms through creating networks of incentives and disincentives, whether by the implementation of social media taxes, as seen in Uganda, or through the use of social credit – looking at a variety of aspects of citizen’s behaviour both on and offline – growing in influence in China.

The legacy of internet shutdowns is chequered. The trend towards using them as a tactic for managing protests really gained traction after their use in Egypt in 2011. As protests against Hosni Mubarak gained steam, the government shut off domestic access to the internet by closing four of the country’s major internet service providers (ISPs) (Richtel, 2011). International media and human rights organizations quickly picked up news of the incident and began advocacy campaigns imploring other countries not to follow suit (Tiku, 2011).

Instances of internet shutdowns appear to be on the rise globally. India is one of the most active and aggressive implementers of internet shutdowns (typically local or regional) where there has been a steady trend upwards from 6 in 2014 to 134 in 2018 to 65 already in the first half of 2019 (Software Freedom Law Centre, India, 2019). Many African governments are increasingly using this technique as well, with the continent witnessing a similarly upward trend with 21 shutdowns in 2018. While India may stand out for the frequency of shutdowns occurring within its borders, a handful of African countries stand out for the duration of their shutdowns. In 2017 and 2018, an internet shutdown that covered the northwest and southwest regions of Cameroon lasted fully 230 days (Access Now, 2019). While in Chad, a blackout targeting social media sites lasted for more than twice that (Adebayo, 2019).
In addition to the work of advocacy organizations, international bodies, most notably the UN Human Rights Council (UNHRC), have spoken up condemning such shutdowns and promoting “the right to freedom of information online” that is based on a 2016 resolution that includes an explicit condemnation of “measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law” (UNHCR, 2016). The African Commission on Human and Peoples’ Rights passed a similar resolution the same year guaranteeing the right to freedom of information online (African Commission on Human and Peoples’ Rights, 2016). But such resolutions have had little impact encouraging the African Network Information Centre – the body responsible for registering African IP addresses – to entertaining (but ultimately not pass) a proposal restricting access to IP addresses and numbers for a year to governments that intentionally limit internet access (Mutung’u, 2017).

Despite vocal condemnation of internet shutdowns, particularly by advocacy groups, the acceptability of some forms of internet shutdowns appears to be on the rise. Some indication of this comes from a recent report from the East African policy centre, CIPESA, which detailed an increased willingness on the part of African governments that ordered internet shutdowns to directly acknowledge them in 2019 over previous years (CIPESA, 2019). Furthermore, in early 2019, there were at least two notable events that signalled this shift. The first being the temporary (and very limited) shutdown of internet access on the London tube in response to the large protest being led by the Extinction Rebellion. The British Transport Police shut down public access to Wi-Fi in the London underground in an attempt to disrupt the protests. The blocking of the Tube’s Wi-Fi, which was not made public before being implemented, was unprecedented. As the British Transport Police argued “in the interests of safety and to prevent and deter serious disruption to the London Underground Network, British Transport Police, has taken the decision to restrict passenger WIFI connectivity at Tube Stations” (Embury-Dennis, 2019). This is certainly more limited than a nationwide disruption to the internet but it is notable because the British government appears to now be flirting with a tactic that it previously had been so critical of, and saw themselves at the forefront of developing a “no internet shutdown norm”. Only a year ago, the British government led the Commonwealth in issuing a ‘cyber declaration’ that sought to prevent commonwealth countries from curtailing access to the internet, even in the context of unrest (Grigsby, 2018). Response to the temporary internet outage has been limited, frequently sarcastic, and surprisingly muted.

Another more widely watched incident provided another signal of this trend. Soon after the protests in London, horrific attacks occurred in Sri Lanka on Easter Sunday. Coordinated and sophisticated terrorist violence left more than 300 dead. Perhaps unsurprisingly the government of Sri Lanka immediately blocked access to social media sites including Facebook, Instagram, Snapchat, WhatsApp and YouTube. In contrast with previous internet shutdowns, there was muted outrage and even significant positive commentary by tech activists writing in liberal media such as The Guardian (Wong & Paul, 2019) and New York Times (Swisher, 2019). A handful of those that often would be the first to condemn the shutdown were acknowledging that the government might have made the right decision. Some began to acknowledge that the risks of misinformation and incitement to violence posed by social media were great enough that they outweighed the potential harm caused by shutting down the social media sites.

These two recent instances also reflect a growing frustration with how difficult it is to control extreme speech on social media and the perceived inaction and inability of large companies to effectively address this challenge. The justifications governments are making in terms of national security and stemming greater violence are increasingly having more resonance, and
those that might have previously been highly critical, even 6 months prior, are now acknowledging that the governments might not have any other choices (Wong & Paul, 2019). The days when social media platforms were touted for their assumed peace-making abilities, whether by bringing warring parties into dialogue (as Mark Zuckerberg claimed was the case with the FARC in Colombia) (Reyes L, 2015) or through the Facebook Safety Check where users flag themselves as safe during violence or a natural disaster, have passed. While in murkier and potentially more complicated territory, we see this changing debate as both healthy and necessary. Not because we agree with the particular stand that shutting off the internet during an attack, as in the case of Sri Lanka, is the right decision; but rather because we believe more nuanced debate is deeply needed. In particular, we would like to see a broadened debate that takes us away from the previous polarization pitting civil society and human rights advocates and social media companies on the one side against governments on the other, and instead towards a debate that takes into account the very real challenges many states face about how to protect the safety of their citizens at the same time as protecting human rights.

While the increase in instances of internet shutdowns in Africa are rising, the limited scope of the existing research about them is notable. This is particularly the case for research that looks in-depth at the social, political, economic, and legal contexts in which internet blockages are embedded and the very different types of shutdowns that occur. The work of advocacy organizations serves an important function in increasing public awareness, but the debate on this complex issue requires more nuanced and time-consuming research than many advocacy organizations have the resources to do. Such research could not only help advocacy organizations, but also policymakers grappling with building regulatory frameworks to keep up with the rapid technological advancements happening around the world.

With the urgent need for more research in this area in the African context in particular, a workshop on Internet shutdowns in Africa was jointly convened by the University of Oxford’s Programme in Comparative Media Law & Policy at the Centre for Socio-Legal Studies and the University of Johannesburg’s School of Communication in 2018 in Johannesburg under the European Research Council’s ConflictNet project. It hosted two dozen participants across the continent representing a wide array of academic disciplines and practitioner fields, including from law, communications, and computer science disciplines, and from the legal, advocacy, and technology sectors. The panels, spread across two days, touched on the most salient issues shaping the modern landscape around shutdowns including the role of social media and elections, the unique demands of internet connectivity in conflict zones, the diverse effects and causes of internet shutdowns and the motivations of governments that have considered but not necessarily implemented a shutdown.

This report reflects on the presentations and discussions to provide a sense of the scope of the current debate around internet shutdowns and to identify both the most pressing themes within those debates and the gaps where further research is most needed. By drawing insight from the comparative analysis afforded by this workshop, we also draw attention to controversial questions that deserve revisiting and challenge some of the assumptions ingrained in the current debate.
What actually constitutes an internet shutdown can be deceptively complex, and the barrier between a shutdown and a disruption can be far less clear than most definitions suggest. The main advocacy organizations have varying approaches in line with their agendas. Access Now, for example, describes an internet shutdown as: “an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information” (Access Now, 2018). Internet shutdowns can be total (as we most often speak of in this report, where there is a blackout or all internet services are silenced) or partial (for the latter only certain websites or applications are blocked) (Internet Society, 2017). Both of these approaches stress intentionality—usually governments but it may also be other actors.

For example, while the Internet Society includes blocking of individual websites or applications, it does not appear to include social media company directed takedowns of content on its platform, actions that are often difficult to detect from outside the company. At a discursive level, these companies explain that this content removal is necessary to reduce hate speech and incitement to violence online, which may seem a more plausible justification than those that may be given by governments claiming to be protecting quite broad concepts like “national security”, when they shut down an entire platform. Certainly, these justifications are qualitatively different; looking at them together highlights the ambiguity and the nuances in shutdowns.

Embedded in these advocacy definitions is also an expectation that the actor perpetrating the shutdown is “usually a government” (Access Now, 2018). Less obvious perhaps is the assumption in much of the discourse that shutdowns are typically perpetrated by governments against their own citizens. Yet, cyber-attacks that attempt to take down particular content or systems can just as readily be perpetrated by foreign governments or even rogue hackers.

In this report, we adopt an approach that attempts to be nuanced and inclusive of the many varied forms a shutdown can take. There is much existing work that tracks instances of internet shutdowns including their duration and location (Access Now, 2018; The Tor Project, 2016), their economic impact (CIPESA, 2017; Leberknight & Raveendran, 2018), and how to use VPNs to circumvent them (Access Now, 2016; Mou, Wu, & Atkin, 2016). What is still needed is more detailed technical, political, and legal analyses of exactly how internet shutdowns are effected and how different they can be. The pan-African comparative perspective afforded by the Johannesburg workshop brought into sharp relief just how varied shutdowns—even those that would fit squarely within Access Now’s definition—can be. Looking at three examples presented during the workshop in contrast illustrates this.

In Cameroon, internet access in the northwest and southwest regions of the country was intermittently slowed down or shut off completely between January 2017 and March 2018 (Dahir, 2018). These regions are also home to the country’s minority Anglophone community, a minority which have been pushing for secession from the rest of the country. One particular period of complete shutdown reportedly lasted over three months forcing many in the region to travel to the francophone part of the country in order to access the internet.
Meanwhile in Zimbabwe in 2016, while Robert Mugabe was still president, the popular social media messaging service was shut off for half a day in the capital of Harare coinciding with a series of anti-government protests (Shapshak, 2016), while in December 2017 the internet and phone lines went down for a day nationwide. In a third more recent incident in January 2019, during protests in response to the lack of change under the new president Emmerson Mnangagwa, the government repeatedly shut off the internet nationwide, ending only when the High Court issued an interim ruling saying that the government had overstepped its mandate in doing so (Dzirutwe, 2019). The government offered no explanation for either the first or the most recent incidents, but explained that the second had been caused by a tractor severing a cable in South Africa. Some observers doubted this explanation and claimed that the shutdown’s timing following closely the coup that deposed Robert Mugabe was no accident.

Finally, take the case of Ethiopia where the government has employed numerous different types of shutdowns over the last few years. In 2016, access to social media platforms specifically in the Oromia region was shut off four separate times, while mobile internet was blocked entirely for a few days in the capital. Later in 2017, internet access was restricted entirely for a day in October, while most social media sites excluding WhatsApp were blocked in December.

While the instances in each of the three countries might for the most part fall under Access Now’s definition of an internet shutdown (perhaps with the exception of the tractor accident in Zimbabwe, if that explanation is believed), they are vastly different in quality. This kind of case study comparison discussed during the workshop highlighted that internet shutdowns should be seen as a spectrum rather than an on/off switch.

Through the workshop discussion, five key dimensions of this spectrum were identified: duration, breadth, depth, speed, and frequency. Frequency and duration are perhaps obvious, representing how often the internet is shut off in a country and how long it is shut off for respectively. Breadth, depth, and speed require more specificity. By breadth, we mean how many people are affected or how geographically dispersed a shutdown is. By depth, we mean what kind of content is targeted, ranging from an entire internet blackout, to particular platforms or even individual users being targeted. By speed, we mean to show a range from slowdowns all the way to full blackouts. While a slowdown may seem distinct from a shutdown, often it renders the internet inaccessible in any meaningfully practical way.

The cases above help to illustrate this spectrum: While the shutdowns in Cameroon were extreme in their duration, they were regional in their breadth and not nationwide, and over time they varied in speed from slowdowns to full blackouts. While those in Ethiopia were frequent in their occurrence, they were even narrower in their breadth sometimes limited to a single city, and relatively limited in their depth targeting individual social media platforms. Finally, in Zimbabwe both instances were quite brief in their duration, but the two differed in depth and breadth. And the technique involved in the shutdown (or slowdown) can also have an impact on the above-mentioned dimensions. For example, during the workshop one participant introduced a case where mobile voice and data prices had been dramatically increased in Zimbabwe in January 2017 coinciding with popular pressure for democratization. A price hike may, like a slowdown, make internet practically impossible for many.

By seeing internet shutdowns as a spectrum rather than in absolute terms, important questions become more apparent, such as why one form of internet shutdown or censorship may be adopted in favour of another. It also forces attention on the wide variety of socio-political,
cultural, and economic context in which shutdowns take place.

In some respects, the public discourse around internet shutdowns is slightly removed from larger discussions about national security or censorship (from targeted requests to take downs of particular content, and from criminalizing content and imprisoning bloggers to targeted hacks or cyberwarfare). Many participants agreed that rather than treating shutdowns as practices that are distinct from other forms of censorship, we should treat them as particularly extreme form of online censorship. We suggest that doing so could help bring internet shutdown dialogue more into conversation with wider discussions about online censorship and information control tactics.
One of the goals of much of the grey literature – and even some of the academic literature – on internet shutdowns is to find ways in which to persuade governments not to adopt shutdowns as a technique to manage information flows. Advocacy organizations have historically taken a rights’ based approach, arguing that internet shutdowns should not occur because of the impact on freedom of speech and access to information. However, a more recent tactic that has received considerable attention has been the economic impact approach. Having found many governments unresponsive to free expression arguments, organizations like CIPESA and the Brookings Institute have looked for arguments that are hoped would be more persuasive (CIPESA, 2017; Kathuria, Kedia, Varma, Bagchi, & Sekhani, 2018; West, 2016). Such approaches are often grounded in the assumption that governments ordering shutdowns are doing because they “are unaware of the full magnitude and consequences of these actions on their economies and citizens” (CIPESA, 2017, p. 6). The Brookings Institute, for example, has argued that such shutdowns cost countries more than $2 billion in 2015 (West, 2016).

Wairagala Wakabi, executive director of CIPESA who had been involved in the CIPESA study, and participated in the Johannesburg workshop, showed how their report attempted to build on previous methodologies from Brookings and Deloitte (2016) to look not just at the direct economic impact but also the indirect impact. This includes factors such as the loss of domestic and international investor confidence as well as the higher cost of doing business without the internet now that many African economies have become reliant on it. As Wakabi explained, CIPESA’s study was an attempt to engage more stakeholders in the discussions about internet shutdowns. Not only government officials, but internet service providers (ISPs) and mobile network operators (MNOs) that had been absent from much of the dialogue.

During the discussion at the workshop, many participants agreed that these kinds of economic studies were an important step to move beyond the rights’ based approach and reach more stakeholders for whom issues other than human rights tend to take priority. However, others raised questions about whether the methodologies employed were able to accurately measure something as complex as the broad economic impact of what is essentially non-access or non-use. Others argued that even an economic perspective might not matter to some stakeholders, particularly when concerns of national security, violent conflict, or terrorism are at the forefront (and have their own economic impact). Furthermore, some argued, neither the human rights-based nor the economic arguments may be relevant to every sector of the public, particularly poor communities. This raised the important – and as yet largely unanswered – question of how much an internet shutdown really affects the poor, particularly those in rural communities with limited prior access to electricity or limited literacy levels.
Beyond the moving stories about the challenges faced by citizens during internet blackouts collected by human rights organizations, there is a need for in-depth research about the complex array of socio-political impacts brought about by internet shutdowns.

One area within this that has received some attention from researchers has been the relationship between access to the internet or social media and protests, social movements, and conflict (Gohdes, 2018; Muller & Schwarz, 2018; Shapiro & Siegel, 2015). Such research more often looks at the impact of having internet access on the success of social movements or the likelihood of conflict, but it can help inform our understanding of the impact of shutting off the internet as well. It is especially relevant in contexts where governments use the reduction of prevention of violence to justify a shutdown.

Much of the research in this area predates the rise in concern about intentional internet shutdowns. Instead, it emerged in the period of optimism about the role of mobile phones and internet access in facilitating pro-democracy social movements – social movements that now often trigger internet shutdowns – that came with the Arab Spring. More recently, as the optimism around the Arab Spring began to fade, more restrained pieces were published that show a complex, and often unclear, relationship between internet and social media access and social movements and conflict.

The literature is mixed, as one special issue of the Journal of Peace Research on communication, technology, and political conflict highlighted. Many of the articles showed conflicting results in the relationship between conflict and technology and internet access, demonstrating how difficult it is to get a clear picture of the relationship between these factors. One article, by two political scientists argued that internet access actually had no effect on the success of pro-democracy movements (Rød & Weidmann, 2015) as many scholars writing about the Arab Spring had believed. Another argued that having access to mobile communications makes it “easier for anti-government actors to coordinate collective action, thereby increasing violence” (Shapiro & Siegel, 2015, p. 312). While yet another piece actually argued that access to social media was more likely than access to radio to lead to incitement to violence (Warren, 2015). Other publications on the topic show a similarly mixed picture. A recent (somewhat controversial) study written by two economists drew a link between having access to social media and instances of hate crimes in Germany (Muller & Schwarz, 2018) while another by political development scholars looking at China showed that blocking previously uncensored material online actually increased exposure to anti-government sentiment (Hobbs & Roberts, 2018). Other research published in the last few years has cautioned restraint when drawing conclusions about the link between internet or mobile phone access and conflict (Brown & Livingston, 2018; Dafoe & Lyall, 2015; Gohdes, 2018; Zeitzoff, 2017), some of which depicted the weaknesses in the research methodologies or overlooked assumptions built into earlier studies.

During the Johannesburg workshop, the importance and often-complicated nature of the role of social media in various situations on the continent was readily apparent. Discussion of the role that social media has played during elections, of how to understand the implications of the spread of misinformation and hate speech on platforms like Facebook and WhatsApp, and of the ethics of restricting access to particular social media platforms, ran throughout much of the workshop.
Elections was a major focus, and during the first panel of the workshop, two computer scientists, Anne Muchiri and Cecilia Nanfuka from the University of St. Paul's Limuru in Kenya showed how access to social media had complicated the electoral landscape in Kenya. While Kenya has not experienced an intentional internet shutdown, its high level of internet penetration and social media activity make it an important case for understanding the relationship between social media and the potential for conflict.

Muchiri and Nanfuka demonstrated how communication between candidates and constituents and among voters was particularly active on the country’s three most popular social media platforms, WhatsApp, Facebook, and Twitter. Much of this communication, Muchiri and Nanfuka argued, led to citizens exposure to fake news. A 2017 Portland and GeoPoll survey showed that 9 out of 10 Kenyans believed they had consumed fake news about the 2017 election (Portland & GeoPoll, 2017), including BBC and CNN news articles doctored to appear to show incumbent President Uhuru Kenyatta decidedly ahead in the polls (CNN and BBC targeted by Kenya fake news, 2017). According to a more recent BBC research paper published in 2018, Kenyans not only believe that fake news is prevalent in their country, but also that there is little they can do to change it (BBC News, Chakrabarti, Rooney, & Kweon, 2018).

In their presentation, Muchiri and Nanfuka demonstrated the influential role that prominent bloggers played in the circulation of fake news. Many were involved in spreading these and other pro-Kenyatta and anti-Odinga messages on their blogs and through the social media accounts. This is particularly concerning when read in tandem with the BBC paper that found that in order to attempt to verify the legitimacy of news received, most Kenyans looked first at the source and the sender of the news (BBC News et al., 2018). When sent by an influential or respected blogger, fake news could more easily make it through this ad hoc screening process.

While the potential for fake news to be spread on social media is concerning, the discussion that followed Muchiri and Nanfuka’s presentation at the end of the panel raised important questions about how influential social media platforms really are in Africa, particularly outside of the main urban hubs, and about digital literacy around identifying and circulating misinformation. The Kenyan case seemed to indicate the problematic potential of social media to increase the dissemination of fake news. While some participants questioned how influential social media really was in comparison to traditional media outlets that still seem to have larger audiences, particularly in rural areas, others argued that stories first published on social media are often picked up by radio and television stations with broader reach. Furthermore, urban residents often pass along news from social media to friends and family in villages who may see their city-dwelling contact as ‘in the know’ and as a result trust the accuracy of the content they share.

One particularly concerning anecdote that arose during the discussion was of the Kenyan habit of adding the phrase “sent as received” to any news content forwarded on WhatsApp. By doing so, participants argued that many Kenyans saw themselves relieved of the responsibility of proving the truth of the content shared, or absolving themselves of being liable for spreading false news or even hate speech or incitement to violence. This has potentially problematic implications for the relationship between misinformation and conflict, leading some participants to point to the importance of digital literacy and training users how to spot fake content.

Another presentation on the impact of access to social media and elections came from Iginio Gagliardone, from the University of Witwatersrand, South Africa. In it, he made a persuasive case that social media can provide an important equalizing function, even when extreme speech
is involved. He presented results from a study led by Oxford’s PCMLP looking at hate speech on Facebook in Ethiopia (Gagliardone, Iginio et al., 2016). Notably, the study found that the large majority of critical statements on Facebook were written by people with little to no influence, measured by the number of followers they had. In this case, such extreme speech seemed to be the result of a sense of disempowerment and inequality and targeted power rather than minorities. In fact, Gagliardone and his collaborators found that the worst comments were posted by people with no followers at all. This, he argued, demonstrated the need to take a more cautious approach to restricting extreme speech. While it is a difficult grey area in which to operate, allowing a certain amount of extreme speech may allow some of those disempowered members of society to feel like they are being heard. Often, preventing the spread of hate speech is used as a justification by some governments when they cut off social media access. While social media is certainly a vehicle for such speech, this presentation provocatively challenged those present to consider that there might be cases in which a certain amount of extreme speech could be acceptable.

Additional scholarship relevant to understanding the social impact of internet shutdowns comes from the field of human computer interaction and looks at the experiences of technology “non-users”. Much of this resides in Western contexts and looks at the motivations and experiences of individuals who intentionally opted out of using certain technologies, like Facebook or video games (Karppi, 2018; Lupien, Grandhi, Plotnick, & Hiltz, 2017; Magee, Agosto, Forte, & Dickard, 2014). In many Western countries, particular following the concern about the impact of social media on political polarization and the spread of misinformation around elections, there has been an increase in public discourse about the value of intentionally disconnecting from social media, allowing users to remove themselves from the online echo chambers. This discourse, and scandals like the one around Cambridge Analytica and Facebook in the US, have begun to change the prevailing Silicon Valley narrative of technology as a panacea to the world’s problems. Academic studies, like one conducted by Seeta Pena Gangadharan, have begun to show how complex exposure to the internet and social media is in countries like the United States, including for disadvantaged populations. In his study, Gangadharan depicts how people from poor underserved communities getting online for the first time were optimistic about the opportunities it afforded but also encountered the negative effects of a “privacy-poor, surveillance-rich” internet (Gangadharan, 2017, p. 597).

By contrast, the literature and the dominant development discourse on technology non-use in the Global South tends to depict it as unintentional, a result of economic or social constraints on the poor (S. Wyche & Baumer, 2017; S. P. Wyche, Schoenebeck, & Forte, 2013). These structural factors are seen as leaving these populations on the wrong side of the “digital divide”. In this context, the Silicon Valley narrative of technology as inherently a tool for good continues to exert power with very few willing to write about the negative impact of technology exposure in places like Africa for fear of empowering governments looking for an excuse to inhibiting ongoing efforts to “connect the unconnected”.

Overall, the discussion during the Johannesburg workshop led to an agreement that research into the impact of internet shutdowns, particularly the relationship between social media and conflict is far from complete. While these presentations and much of the existing research in this area discuss the impact of having access to the internet and social media, rather than being denied access during a shutdown, they are nonetheless vitally important for any chance of fully understanding, even if indirectly, the impact a shutdown might have. And crucially, exactly who
(or what segment of the population) a shutdown is targeting (e.g. those wealthy enough to have access to social media, often in urban areas, and frequently of a younger demographic). When countries like Cameroon and Ethiopia choose to target social media platforms for censorship rather than the entire internet, efforts like those from Gagliardone and Muchiri and Nanfuka to better understand the role of social media in conflict-prone environments become both necessary and urgent. Discerning the impact of access to social media and the internet on populations is an endeavour still very much in the early stages of research, regardless of context. Building on this work, particularly in understudied contexts, is vital for constructing a more holistic understanding of the impact of intentional internet shutdowns.
Since 2016, Access Now has collected data in their “Shutdown Tracker Optimization Project” about not only when the internet appears to be shut off in a particular country, but also what justification was given by the authorities for the shutdown, what region was affected, what legal method was used, and what events (like protests) coincided with a particular shutdown (2017). What emerges is how varied the justifications given can be, particularly in Africa. On more than one occasion, the Zimbabwean government, for example, attributed an internet or social media blackout to technical problems, sabotage, or third-party involvement, removing themselves from responsibility for the block. By contrast, in Ethiopia, during its shutdowns in 2016 and 2017, the government accepted responsibility but explained that they were necessary in order to prevent cheating and distraction during the school exams. Other countries like Togo, the Democratic Republic of Congo, and Uganda, have used more “traditional” justifications, like preventing the spread of rumours and illegal information or protecting public safety and national security.

Some research has attempted to unpack these justifications. For example, in an early study on the subject published in 2011, Philip Howard and his co-authors tracked justifications given for shutting off access to social media in 566 separate instances that had occurred around the world since 1995, with a focus on differences between autocratic and democratic regimes and noted “both democratic and authoritarian regimes disable social media networks citing concerns about national security, protecting authority figures, and preserving cultural and religious morals. Whereas democracies disable social media with the goal of protecting children, authoritarian regimes also attempt to eliminate what they perceive as propaganda on social media” (Howard, Agarwal, & Hussain, 2011, p. 216).

More recently, Patricia Vargas-Leon looked at shutdowns between 2005 and 2015 and found a difference in how democratic and “hybrid” regimes justified their actions. When considering a shutdown, “democratic regimes...emphasized the protection of critical infrastructure in case of a cyber-attack;” when actually implementing one, they “claimed it was an accident and denied their intention to use it for political purposes” (Vargas Leon, 2016, p. 4). By contrast, she found that hybrid regimes would “blame foreign powers for the instability of their regime and claim an ‘unclear’ national interest threatened by the internet” (Vargas Leon, 2016, p. 4).

Research that has focused on particular cases illustrates the variety of contexts in which justifications are given. For example, in Ukraine amidst its ongoing conflict with Russia over the sovereignty of Crimea in 2017, President Poroshenko ordered a blanket ban on Russian-run social media and search engine services for three years. In an article that looked at – and questioned – the legality of such a move, legal scholar, Natalie Holland showed how Ukraine justified this ban pointing to “Russian propaganda, data collection and cyber attacks” (Holland, 2017, p. 948). Moreover, Holland acknowledged that some of the sites specifically targeted by
the Ukrainian government did publish clearly pro-Russian content and failed to take down overtly violent anti-Ukrainian posts. So, according to Holland, while the justification given maybe have been insufficient, it was rooted in truth.

Similarly, helpful cases were discussed during the Johannesburg workshop. For example, Martial Sylvain Marie Abega Eloundou from the Catholic University of Central Africa, presented the case of the extremely long shutdowns in Cameroon. Like some of the authors above, Abega Eloundou took a communications approach and looked at how the Cameroonian government justified its action. By examining public appearances of prominent government officials – including speeches and interviews – Abega Eloundou identified the main justification given for the shutdown, namely preserving “public order”. Abega Eloundou showed how Cameroonian government officials frequently cited the Rwandan case of Radio Mill Collines to argue that separatists could easily influence social media content, which could lead to public unrest or even violence. Like the hybrid regimes in Vargas-Leon’s study, the Cameroonian government cited relatively opaque national security concerns. However, more like the authoritarian regimes in Howard’s study, the goal appeared to be reducing perceived propaganda from a separatist group on social media.

In addition to the case of Cameroon, the Johannesburg workshop included a full panel on justifications given for shutdowns with presentations covering Ethiopia, Zimbabwe, and Uganda.

Yohannes Eneyew Ayalew, an Ethiopian legal scholar from Samara University, presented the case of Ethiopia. There, the government typically justified its frequent shutdowns between 2016 and 2018 as necessary to protect national security or to prevent students from cheating on their exams. Yet, Eneyew Ayalew showed how some of these shutdowns coincided with the Amhara protests, Ethiopia’s second largest group.

Next, Chris Mhike, a lawyer from Zimbabwe, discussed the justifications given by its government around its internet shutdowns in 2016 and 2017, the first of which was limited to social media while the second was a full but brief shutdown. With the first ISP opening in 1994, Zimbabwe has a relatively high internet penetration rate over 50 percent with a very active population on social media, particularly WhatsApp, which accounts for a third of internet data use in the country, according to Zimbabwe’s telecommunications regulator (Karombo, 2018). While the government offered no explanation at all for the social media blackout in 2016, in 2017 it attributed the shutdown to an accident involving a tractor and severed cables. To Mhike, these explanations were dubious at best. “Most people in Zimbabwe don’t buy these explanations,” he explained. Unlike the Ethiopian government, the government in Zimbabwe appeared eager to shift blame for shutdowns away from itself.

In some countries, internet and social media shutdowns are initiated following a direct executive order, at times done unconstitutionally. In others, governments use the law to justify their action. In particular, they often refer to criminal codes or laws pertaining to telecommunications and communications infrastructure. Take the case of Uganda. At the workshop, Dorothy Mukasa, CEO of the NGO Unwanted Witness, told the story of the attempt her organization made to challenge internet shutdowns that took place in Uganda in 2016, the first in February, the second in May. Unlike both Zimbabwe and Ethiopia, the Ugandan government offered legal justifications for the shutdowns. In particular, they cited the Regulation of Interception of Communications Act 2011 and the Ugandan Communication Commission Act (UCCA) of 2012,
which they argued authorized them to shut off the internet to protect national security. Unwanted Witness and another civil society organization, Legal Brain Trust, challenged these shutdowns in courts. Yet the courts quickly dismissed one of the cases on technical grounds saying that they did not “exhaust all remedies”. In the UCCA, there are provisions for an independent tribunal where citizens were meant to bring problems with the Communication Commission, the body that had ordered the shutdown. But that tribunal was never set up, making it impossible for Unwanted Witness to “exhaust” that particular remedy. Even so, the court dismissed the case. As Mukasa argued, the case demonstrated the in Uganda, the government together with the courts would hear cases, but would find legal technicalities with which to dismiss them.

MOTIVATIONS & POWER RELATIONS

The kinds of official justifications governments give when the internet goes down are only a small window into the actual causes. Without knowing everything that motivates the actions of political leaders, attempts to understand fully the causes of shutdowns can easily become politicized or can rely on data that is more circumstantial than definitive. In Access Now’s tracking, they often record the “suspected actual cause” of a shutdown next to the official justification given; as of mid-2018, in 64 percent of the incidents they recorded they noted the “suspected actual cause” to be protests. While protests are indeed often linked with instances of internet or social media censorship, it is difficult to know definitively that they are the “cause” of a particular shutdown.

Some researchers have attempted to bridge this gap between suspected causes and actual causes, typically doing so through comparative quantitative analysis. For example, Sebastian Hellmeier, combined data about instances of shutdowns collected by the Open Net Initiative with a variety of other socio-political factors in 34 autocratic regimes around the world. He found that “monarchies, regimes with higher levels of social unrest, regime changes in neighbouring countries, and less oppositional competition in the political arena are more likely to filter the internet” (Hellmeier, 2016). A similar study conducted by Jan Rydzak looking at internet shutdowns in “non-democracies” showed that they were more likely to occur in countries with higher internet and mobile penetration rates, but that at a particularly high level of penetration even autocratic regimes were less likely to shut down the internet. Moreover, he found that conflict occurring at the domestic or interstate level had no effect on the likelihood of shutdowns, but that conflict occurring in a neighbouring country did (Rydzak, 2015).

Drawing on a more theoretical multi-country comparison in Africa, one presenter at the Johannesburg workshop, Vincenzo Cavallo, founder of the Kenyan-based Cultural Video Foundation, attempted to narrow in on some of the factors that might influence internet shutdowns. In his presentation, Cavallo theorized that it might be possible to identify three key elements in what he described as the ecology of media shutdowns: media penetration, the economy, and the government’s media skills. By including media penetration, he agrees with Rydzak’s findings that higher levels of internet penetration might increase the chance of having a shutdown, but Cavallo suggested that the level of penetration might also influence the depth of censorship adopted – from targeted website takedowns to full blackouts. He also argued that the importance of the internet to a country’s economy could influence the kind of censorship
tactics adopted. He illustrated this with the case of Kenya, where the ICT sector plays an increasingly important role in the economy and where the government decided not to shut down the internet during the 2017 election.

THE POWER OF THE COURTS

Enriching these more removed comparative studies, many of the presentations in the Johannesburg workshop brought a detailed look at the potential causes in individual cases. While the comparison this afforded did not allow for the verification of the specific findings mentioned above, it did generate theories about potentially new factors that might go unnoticed in a quantitative analysis. In particular, in the discussion around the cases of Ethiopia and Uganda, the potential role of the courts and law in relation to executive power was discussed. One participant suggested that the amount of power a government has vis-à-vis the public might influence the kind of censorship it adopts, how it justifies it, or how likely it is to entertain challenges to it. For example, in the case of Ethiopia where the government justified ordering the shutdowns on the grounds of preventing exam cheating and refused to entertain any legal challenges to its decision, the government has authority over the courts. In fact, during one panel discussion one participant even suggested the government was so powerful in Ethiopia that the law did not matter, at least not to the actions of the government (see, also, Stremlau 2018). In contrast, in Uganda when shutdowns occurred the government was compelled to offer a legal justification for the shutdown. While it ultimately blocked the challenges from civil society in the courts, it could not dismiss the challenges outright, as in Ethiopia. Similarly, during the January 2019 shutdowns in Zimbabwe, a High Court ruling that the government had overstepped its mandate in ordering the shutdown resulted in the end of the internet blockage.

THE POWER OF THE PRIVATE SECTOR

Other cases presented suggested there might be more stakeholders able to exert power to influence government censorship decision. One type of actor that came up repeatedly was the role of private sector actors like the Internet Service Providers (ISPs) and Mobile Network Operators (MNOs). Presentations on Burundi and Zimbabwe illustrated this particularly well.

Jean-Paul Nkurunziza, a Burundian specialist in internet governance, presented the case of social media shutdowns in Burundi between April and May 2015 ahead of the presidential election that year. A wave of protests had erupted in the capital after President Pierre Nkurunziza announced he would run for a third term despite constitutional provisions restricting presidents to a two-term limit. The government responded by ordering the ISPs to shut off access to social media platforms, specifically, Twitter, Facebook, Viber, WhatsApp, and Tango. The national regulator invited all the ISP directors to an in-person meeting and ordered them to shut down the platforms. Unhappy with this order, the ISP directors, asked for a written order to verify it. Their demands were dismissed. The regulator said simply that the order had come “from above” and that proof was unnecessary. Ultimately, while the ISPs appeared to want to resist the government directive, they were powerless to do so.

The power relations between the government and the ISPs and MNOs were different in the case of Zimbabwe, as presented by Admire Mare from Namibia University of Science and Technology.
Mare showed how unique the relationship was between the Zimbabwean government and one of the country’s MNOs, ECONET Wireless, around the shutdowns in 2016 and 2017. Out of the three main MNOs in the country, the government fully owned one and owned a majority stake in a second, while the third, ECONET was completely private. In many countries, being completely private would not fully inhibit a government’s power over a private internet company. The government could still restrict – or threaten to restrict – licenses, a serious concern for any private company in the media sector. However, ECONET’s position is somewhat different. Not only is it the largest of the three telecommunications providers in the country, it is also one of the largest companies on the country’s stock exchange and was the first of the three to launch 3G data technology in 2009. While ECONET was created in Zimbabwe, it has since expanded to other African countries, including Burundi and the Central African Republic, and has even acquired one of Zimbabwe’s banks. Mare discussed how, with this position of relatively power in the Zimbabwean economy, ECONET’s power vis-à-vis the government was much stronger than most. As a result, it has been able to challenge some government censorship directives. However, without being present in the negotiations between ECONET and the government it is impossible to know how much push back is possible. The government could still restrict its license at any time. But with its powerful position in the economy ECONET is more protected from this than most ISPs.

Together, the cases of Burundi and Zimbabwe provided a convincing indication of the importance of including ISPs and MNOs in any analysis that looks at the power relations between the government and other societal actors influencing internet censorship. It also highlights how important international market dynamics around social media firms can be for understanding why particular internet censorship tactics have been adopted (Pan, 2017). Similarly, accounting for the ownership of the internet infrastructure, and the relationship between the state and ISPs, in a particular context is important to understanding the mechanisms at the state’s disposal for control, either direct or indirect (Freyburg & Garbe, 2018, p.3896). In a literal way, “who controls the pipes” can play quite an important role in what internet censorship in a particular country looks like.

THE POWER OF TRADITIONAL MEDIA & THE PUBLIC

One of the unique aspects of the conversations in the Johannesburg workshop turned out to be the inclusion of countries that have opted not to completely block social media and the internet. Wambui Wamunyu, from Daystar University in Kenya, presented her work on the Kenyan government’s approach to curtailing access to information after the controversial 2017 presidential election and subsequent protests in 2018. Perceived election irregularities led to the High Court ordering a second election be held two months later. Frustrated by the lack of progress, opposition candidate, Raila Odinga, boycotted the vote and in 2018 held his own “swearing in ceremony” in protest. Wamunyu’s research looked at the events surrounding the 2018 swearing in protest. Ahead of the protest, the government warned online media and broadcast television about covering the event. When the media outlets covered it anyway, the government shut off the broadcast towers turning the television sets black. Yet the government did not shut off the internet. Participants suggested the relative power of traditional versus new media might play a role. While social media is increasing in influence, particularly among more affluent Kenyans, television still has the broadest reach (Communications Authority of Kenya,
Moreover, the internet has an important role to play in Kenya’s growing ICT sector, particularly in the banking sector with the prevalence of mobile banking platform like MPESA. Thus, Wamunyu argued, the preference for restricting television, was in part because of a combination of the influence of television on popular opinion and the influence of the internet in the economy.

In some instances, concerns about domestic public opinion influence governments’ approach to censorship. For example, during the workshop, Shepherd Mpofu from the University of Limpopo, showed how the Zimbabwean government’s concern about domestic public opinion led it to choose more subtle ways to curtail internet access than outright blackouts. His presentation revolved around one incident back in 2015 during Robert Mugabe’s presidency when he appeared to fall on some stairs on his way to a podium to give a speech. Quickly, Mpofu explained, the government launched an initiative on Twitter and other social media platforms to spin the incident as one in which Mugabe almost fell, but instead saved himself at the last minute. The incident also coincided with a weeklong increase in the price of data. While this price hike would not traditionally be considered an internet shutdown, for many it made the price of data untenable and the internet therefore much harder to access. Mpofu’s presentation gave some indication that in cases where public opinion is a concern, government’s may opt for more subtle forms of information control.

Another presentation, this time from Renaud de la Brosse, from Linnaeus University in Sweden, showed how the same may also be the case for governments concerned about international public opinion as well as, or perhaps even more so than, domestic public opinion. In his presentation, de la Brosse presented the case of Morocco, which he described as a “communicating state” that cares deeply about its international reputation and this was a reflection of how important international tourism was to its economy, making up fully 8 percent of its GDP (Oxford Business Group, 2018). As such, Morocco strives to maintain its reputation as both a desirable tourism destination and a moderate Western-friendly country in the Arab region. Tourism is understandably quite sensitive to changes in international public opinion. To date, the Moroccan government, led by King Mohammed IV, has, like Kenya, chosen not to censor the internet. However, it has still worked in more subtle ways to restrict free speech and especially speech critical of both the King and his administration. For example, de la Brosse argued, the Moroccan government is frequently engaged in defamation suits against journalists who criticize the government, cases that often result in heavy fines that are difficult to appeal. This in turn leads to self-censorship in the newsrooms. It also exerts pressure through threatening to withhold advertising. With the King as the most important businessperson in the country, losing his advertising revenue could be very problematic for a traditional news outlet.

During the discussion that followed, the importance of international public opinion in the Kenyan case emerged as well. As Wambui explained, Kenya has invested quite a lot in the “Brand Kenya” initiative, which features international tourism prominently. Tourism makes up just under five percent of Kenya’s current GDP; its reputation as a safari destination is an important factor in that. The discussion also revealed how Morocco’s reliance on international public opinion goes beyond the tourism industry. De la Brosse talked about how poor most people in Morocco were and how reliant the country’s economy was on foreign investment even outside of the tourism industry. Data from the United Nations Conference on Trade and Development (UNCTAD) confirms this. As of 2016, foreign direct investment equalled over 50 percent of Morocco’s GDP making the government highly sensitive to changes in international public opinion (Santander, 2018).
In much of the public discourse about internet shutdowns, the focus tends to be squarely on the government as the perpetrator, the actor that is directly responsible for causing a shutdown. Yet it is readily apparent that the array of actors who might cause an internet outage is far broader. From accidental power and internet outages caused by severe weather like hurricanes to distributed denial of service attacks in “cyber warfare”. Governments are not the only actors who intentionally try to restrict access to the internet or certain content on it (Herzog, 2011; Mueller, 2017). Hackers working for terrorist organizations or even just internet trolls can play an important and often unseen part in restricting access to certain content. Even private companies play a role here. ISPs have been known to at least slow down internet access at times or for certain content, a particular concern in the ongoing debate around net neutrality (Marsden, 2016). Similarly, social media companies now have growing departments tasked with identifying and taking down hate speech or “inappropriate” content from their platforms.

Sometimes, like in the case of severe weather, internet shutdowns can be caused by factors beyond any one actor’s control. Kenyi Yasin Abdallah Kenyi, a legal practitioner from South Sudan, provided a key example of how this is the case in situations of ongoing conflict. South Sudan’s three main ISPs have all rolled back plans to expand access following the intensification of violence in 2015 due to the higher risk associated with constructing and operating infrastructure in conflict zones as well as falling subscriber numbers even where they have been able to reach. The availability of internet access is further restricted due to the high cost of theinternet that is available. South Sudan is a landlocked country meaning that it lacks direct access to underwater fibre internet cables. Furthermore, due to the ongoing conflict, plans to lay an underground fibre backbone connecting it to countries that do have such underwater fibre, like Djibouti, Kenya, or Tanzania, have been repeatedly announced and then abandoned due to the conflict making such construction challenging. As a result, all South Sudanese ISPs rely on either direct satellite connections or microwave links to satellite connections in neighbouring countries, both of which are expensive (Garcia & Kelly, 2015).

In other cases, like Zimbabwe, governments at times blame shutdowns on factors outside of their control. With reports of earthquakes severing cables in Hong Kong (Wai-yin Kwok, 2006), a woman accidentally cutting a cable while digging for copper in Georgia (Chang, 2013), and monkeys causing power outages after tripping transformers in Kenya (Obulutsa, 2016), a tractor severing a cable, as the Zimbabwean government claimed, is certainly not impossible. Determining whether a particular shutdown was indeed an accident is a clear challenge.

Kenyan legal scholar, Robert Muthuri, presented his ongoing work to try to do just that in the Kenyan case. To begin, Muthuri used Network Diagnostic Tests developed by the Open Observatory of Network Interference (OONI) to measure connectivity speeds in Kenya for the month of October 2017 around that year’s repeat election. He found that the speeds of both uploading and downloading were reduced on election day, 26 October 2017.
(Muthuri, 2017). This finding could have led to a quick conclusion that the government had intentionally ordered the ISPs to slow connectivity speeds in order to reduce the potential for opposition protests around the election. However, taking a more cautious approach, Muthuri emphasized that their data said nothing about the intentionality of the slow-down, only that it had occurred. For example, as he explained, while intentional government pressure may be one potential cause, it could also have been unintentional, caused by increased traffic online with more users wanting to communicate urgently around the controversial political event. Similarly, it could also have been the result of intentional throttling on the part of the ISPs, who, he suggested, might be throttling for various profit-maximizing motives. In the end, Muthuri’s illustration provided a strong case for the need for his and others’ ongoing work to development better tools to identify both the actors involved and the intentionality of internet blockages.
All the discussion of the varied contexts in which African internet shutdowns take place raised a number of important – and at times controversial – questions about the norms surrounding shutdowns and the acceptability of a shutdown particularly in the context of a large-scale terrorist attack or the persistent use of social media in genocide.

Looking at the justifications actors often give for initiating shutdowns, many point to the law, particularly law around communications and terrorism to legitimize their actions, particularly in the interest of protecting national security or fighting terrorism. However, the law has a reputation for lagging behind technological development it might seek to regulate. Even the highly publicized adoption of the General Data Protection Regulation in Europe took two years to integrate fully into member countries’ legal systems, by which time the Cambridge Analytical scandal and a number of data breaches had taken place. In 2016, the UN Human Rights Council passed a resolution reaffirming the protection of human rights in the digital space and condemning efforts to disrupt access (United Nations, HRC, 2016), but the state of international law governing access to online information is far from definitive.

Some legal scholars and organizations (Council of Europe, 2017; Weber, 2011) have attempted to address this lack of legal framework around the right to internet access by drawing from existing international law around control of the sea and of space to outline the responsibilities government should have to protect the internet, particularly when its restrictions might infringe upon the sovereignty of another state. Others have used analyses of domestic laws to attempt to argue that internet shutdowns are not only illegal but also a poor choice in response to, for example, social uprisings (Yang, 2012). At the Johannesburg workshop, Eneyew Ayalew attempted a similar endeavour in his presentation, arguing that Ethiopia’s shutdowns were outside of both international and domestic law.

While the public debate about internet shutdowns largely agrees with this position about the illegality of any form of internet shutdowns, some participants raised important ethical questions that challenged these assumptions.

For example, Abega Eloundou argued that more needs to be done to find a fairer way in which to balance the need to respect the right to access information and the responsibility states have to prevent conflict and violence. Abega Eloundou used the case of Cameroon to illustrate how governments often lean too quickly in favour of preventing violence than protecting speech when making this decision. In Cameroon, he explained the government failed to take into account the ability of its citizens to judge the quality of the messages they receive. Nonetheless, he argued that popular discourse about internet shutdowns downs tends to overlook the challenges involved in making decisions about these kinds of trade-offs.

This led to concerns about the need to prevent the spread of things like hate speech, incitement to violence, and misinformation, and to assist in ending ongoing conflict, or to restrict the ability of truly violent separatist or terrorist groups from recruiting or carrying out violent campaigns. While these
responsibilities frequently appear in the official justifications given by governments that initiate what are clearly disproportionate crackdowns on opposition groups, there are times when these responsibilities are very real and legitimate concerns.

Kenyi’s presentation of South Sudan showed how, since the outbreak of violence in 2015, the South Sudanese government has requested the shutdown of communication connections in certain parts of the country. In one instance, for example, this was relatively narrow in breadth and targeted the Upper Nile region where the government was at the time launching military operations into rebel held territories. In another, the government restricted internet services in the capital, Juba, after soldiers defected from the military and launched attacks on the outskirts of the city. While the government in this case balanced similar issues to those in other countries – namely the prevention or reduction of violence versus the respect for freedom of information – many other participants in the workshop agreed that the government was more justified than most in its action because of how present the threat of conflict was and how limited internet access was to begin with beyond rebel groups. Whether one agrees with them likely depends on whether or not you see the South Sudanese government as legitimate in the first place or support their reasons for going to war.

Cases like South Sudan raise yet more questions about who ought to judge whether a particular type of shutdown is necessary/useful/justified. Governments have so far been the most prominent actors making these decisions, but they have also been the ones most targeted for abusing that power. In other cases, it is not just governments making these decisions for us, but ISPs and social media networks too. Unlike at least some governments, private companies have little accountability to the public and insufficient transparency about how decisions are made that govern the content we see and can access.
As technologies continue to change, it is likely that internet censorship will not look like the “internet shutdowns” we know today. In particular, as governments gain technological expertise and surveillance capabilities improve, it is likely that there will be a move away from the particularly blunt instrument of internet shutdowns – whether national or local – instead choosing an array of tactics that vary more greatly in depth, breadth, speed, and perhaps along other unforeseen dimensions. Public discourse in the media and by advocacy groups on shutdowns tends to present it as a mechanism detached from other more moderate forms of information control. And with the perceived severity of the impact of a full internet blackout, perhaps shutdowns do deserve to be treated as such. However, doing so risks removing shutdowns from ongoing and quickly evolving debates about the impact of pressing concerns such as hate speech, incitement to violence, and misinformation online and its connection with violence offline. Furthermore, by focusing specifically on government strategies for restricting information access, internet shutdown discussions run the risk of overlooking the role that crucial but less obvious stakeholders such as ISPs, MNOs, social media networks, traditional media outlets, and businesses play in controlling the information we do and do not have access to.

Analysing internet shutdowns as existing on a spectrum – varying along dimensions such as duration, breadth, depth, speed, and frequency – allows that discussion to stay engaged with changing debates about the evolving, and competing, norms governing the internet that may shape the form shutdowns take in the future and the ways in which they are both justified and legitimised.

The discussion held during the workshop demonstrated a need for more research around the impact, the causes, and the effects of internet shutdowns, as well as the whys and hows particular techniques are chosen over others. More research is needed to answer questions about the technological developments enhancing the ability and willingness for actors to resort to shutdowns, the role played by international and non-state actors, and the legal and political processes that both enable and legitimise certain shutdowns.

In terms of the impact of internet shutdowns, analyses looking at the economic impact are notable attempts to shift the debate, but alone are insufficient for assessing the full scope. During the workshop, the importance of conducting research into questions about the more nuanced, and often harder to access, dimensions of socio-political impact became readily apparent. In particular, with limited internet access outside many urban areas in Africa, what is the true impact of various forms of shutdowns on the rural poor? How do people cope or innovate under internet shutdowns? How influential are social media platforms to political decision-making? Even in Kenya with one of the highest internet penetration rates on the continent, broadcast television still appears to be more influential than social media. Many governments choosing to target social media platforms argue that such platforms breed a particular type of hate and incite violence, pointing most recently in particular to its penchant for distributing false information. Discerning the impact of access to social media and the internet on different populations is complex, regardless of context. Building on this work, particularly in understudied regions of Africa, is vital for constructing a more holistic understanding of the true impact of internet shutdowns.
In popular debates about the causes of internet shutdowns, governments are almost always seen as the perpetrators; they are framed as the villains restricting freedoms. Yet existing research and the debate at the workshop show how varied the causes can be – from the unintentional, including severe weather and accidentally severed cables, to the intentional but non-governmental, such as foreign government attacks, rogue hackers, or ISP led slow-downs. While many definitions of what constitutes an internet shutdown expressly exclude unintentional shutdown from the list, it is more difficult than it may seem to tell the difference and it is important to find ways to accurately and reliably distinguish between the two.

Even where governments are the causes, greater consideration of the other actors involved may help enhance understanding of why they make the choices they do. Including, for example, research looking at the role and power of a range of different stakeholders, from the courts to mainstream journalists, sitting government officials to political candidates, domestic publics to foreign publics, and ISPs and MNOs, terrorist organizations and the military. Focusing on the kinds of power relations that exist and how power is exerted between them could provide productive insights into opaque government decision-making processes. For example, why do some government prioritize their international reputation while others do not? And why are some ISPs and courts able to stand up to governments while others are not?

The Johannesburg workshop made one point particularly clear: We need more dialogue that includes as many of the diverse stakeholders as possible. While discussions that take place at international conferences on internet shutdowns (and freedom of speech more broadly) are important, they are rarely attended by those within government that are either tasked with restricting certain types of content, or managing elections, protests or other events that are often associated with internet shutdowns. As a result, there is a gap in discussions about the adoption of particular forms of shutdowns. Engaging with government officials – though difficult – as well as international social media networks like Facebook and Google, local MNOs, and even traditional journalists, is a necessary step towards finding a fair balance between the need to reduce the potential for violence and the fundamental right to freedom of information.


Software Freedom Law Centre, India. (2019). Internet Shutdowns in India. Retrieved from https://internetshutdowns.in


The following is a list in alphabetical order of all of the participants who attended the Internet Shutdowns in Africa Workshop, held in Johannesburg, South Africa, 7-8 June, 2018.

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization/Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>KENYI YASIN ABDALLAH</td>
<td>The Advocates for Human Rights and Democracy, South Sudan</td>
</tr>
<tr>
<td>RENAUD DE LA BROSSE</td>
<td>Department of Journalism, Linnaeus University, Sweden</td>
</tr>
<tr>
<td>VINCENZO CAVALLO</td>
<td>Cultural Video Foundation, Kenya</td>
</tr>
<tr>
<td>SARAH CHUMBU</td>
<td>University of Johannesburg, South Africa</td>
</tr>
<tr>
<td>MARTIAL ABEGA ELOUNDOU</td>
<td>Catholic University of Central Africa, Cameroon</td>
</tr>
<tr>
<td>SARA FINDLAY</td>
<td>Media Monitoring Africa, South Africa</td>
</tr>
<tr>
<td>IGINIO GAGLIARDOE</td>
<td>University of Witwatersrand, South Africa</td>
</tr>
<tr>
<td>EMILAR GANDHI</td>
<td>Facebook, South Africa</td>
</tr>
<tr>
<td>ANNA-MARIE JANSEN VAN VUUREN</td>
<td>University of Johannesburg</td>
</tr>
<tr>
<td>ELEANOR MARCHANT</td>
<td>PCMLP, Centre for Socio-Legal Studies, University of Oxford, U.K.</td>
</tr>
<tr>
<td>ADMIRE MARE</td>
<td>Dept. of Communication, Namibia University of Science &amp; Technology</td>
</tr>
<tr>
<td>CHRIS MHIKE</td>
<td>Atherstone &amp; Cook Legal Practitioners, Zimbabwe</td>
</tr>
<tr>
<td>SHEPHERD MPOFU</td>
<td>Communication Studies, University of Limpopo, South Africa</td>
</tr>
<tr>
<td>ANNE MUCHIRI</td>
<td>Computer Science Department, University of St. Paul's Limuru, Kenya</td>
</tr>
<tr>
<td>DOROTHY MUKASA</td>
<td>Unwanted Witness, Uganda</td>
</tr>
<tr>
<td>ROBERT MUTHURI</td>
<td>CIPIT, Strathmore Law School, Kenya</td>
</tr>
<tr>
<td>JEAN PAUL NKURUNZIZA</td>
<td>Internet Society, Burundi</td>
</tr>
<tr>
<td>ANRI VAN DER SPUY</td>
<td>Researchch ICT Africa, South Africa</td>
</tr>
<tr>
<td>NICOLE STREMLAU</td>
<td>University of Johannesburg &amp; PCMLP, University of Oxford, U.K.</td>
</tr>
<tr>
<td>WAIRAGALA WAKABI</td>
<td>CIPESA, Uganda</td>
</tr>
<tr>
<td>WAMBUI WAMUNYU</td>
<td>Media &amp; Film Studies, Daystar University, Kenya</td>
</tr>
</tbody>
</table>
Programme in Comparative Media Law & Policy

Centre for Socio-Legal Studies
Faculty of Law
University of Oxford
Manor Road Building, Manor Road
Oxford, OX1 3UQ
Tel: +44 (0) 1865 284220
Fax: +44 (0) 1865 284221

For more information, please visit our website at pcmlp.socleg.ox.ac.uk/