Opening and Closing Online Civic Space in Africa: An Introduction to the Ten Digital Rights Landscape Reports

Tony Roberts and Abrar Mohamed Ali

Abstract

This report introduces findings from ten digital rights landscape country reports on Zimbabwe, Zambia, Uganda, Sudan, South Africa, Nigeria, Kenya, Ethiopia, Egypt, and Cameroon. They analyse how the openings and closings of online civic space affect citizens' digital rights. They show that:

a. When civic space closes **offline** citizens often respond by **opening civic space online**.
b. When civic space opens **online** governments often take measures **to close online space**.
c. The resulting reduction in digital rights makes it **impossible to achieve** the kind of inclusive governance defined in the Sustainable Development Goals (SDGs).

We know far more about openings and closings of online civic space in the global North than we do in the global South. What little we do know about Africa is mainly about a single country, a single event, or single technology. For the first time, these reports make possible a comparative analysis of openings and closings of online civic space in Africa. They document 65 examples of the use of digital technologies to **open** online civic space and 115 examples of techniques used to **close** online civic space. The five tactics used most often to close online civic space in Africa are digital surveillance, disinformation, internet shutdowns, legislation, and arrests for online speech.

The reports show clearly that any comprehensive analysis of digital rights requires consideration of the wider political, civic space, and technological contexts. We argue that countering the threats to democracy and digital rights discussed in the reports requires new evidence, awareness, and capacity. We propose applied research to build capacity in each country to effectively monitor, analyse, and counter the insidious impact of surveillance and disinformation; and a programme to raise awareness and mobilise opinion to open civic space and improve citizens' ability to exercise, defend, and expand their digital rights.

DOI: 10.19088/IDS.2021.005

1. Introduction

Civic space remains open in only two of Africa's 54 countries,[1] according to CIVICUS (2020). The reduction in safe public spaces in which democratic debate can take place represents a breach of citizens' digital rights and makes achievement of the Sustainable Development Goals (SDGs) impossible. This report presents the literature review used by the African Digital Rights Network[2] to provide the conceptual framing for the commissioning of digital rights landscape country reports on ten African countries. It also presents preliminary findings and makes tentative recommendations designed to enhance the ability of citizens to exercise, defend, and expand their digital rights.

Civic space refers to the public places where citizens can freely exercise their human rights. This includes the right to freedom of opinion and expression. Civic spaces can be **offline** physical locations, such as village halls or public squares, or **online** virtual spaces for digital discussion, online petitions, or hashtag campaigns. Online civic space can provide a refuge for marginalised or opposition groups, particularly in offline contexts where such voices are disciplined or oppressed. Civic space is crucial for any open and democratic country in which citizens and civil society are free to hold power-holders accountable, draw attention to neglected issues, and foster inclusive decision-making at all levels (Kode 2018).

Digital rights are human rights in online spaces. These rights include, but are not limited to, the right to privacy, freedom of opinion and speech, freedom of information and communication, gender rights, and the right to freedom from violence (APC 2006; Abraham 2014; UN 1948). Citizens' digital rights are breached if they are the subject of digital surveillance; if they are covertly targeted with disinformation to manipulate their beliefs and behaviour; if their mobile or internet connection is restricted; or if they are arrested or attacked for expressing political opinion online (Jorgensen 2006; GISWatch 2014; GISWatch 2019; Zuboff 2019). Examples of digital rights breaches include online gender-based violence perpetrated by misogynist groups; mass interception of digital communications by state spy agencies; or private sector actors trading citizens' digital profiles to enable covert voter disinformation campaigns.

As governments close civic space *offline*, citizens often open civic space *online* (Buyse 2018; Roberts 2019). Mechanisms used to close offline civic space have included laws, regulations, limits on funding, threats and

[1] The two island states of Cabo Verde and São Tomé and Principe.

[2] **African Digital Rights Network**.

©2021 Tony Roberts & Abrar Mohamed Ali ©Institute of Development Studies. DOI: 10.19088/IDS.2021.005

violence, arbitrary arrest, and detention (Dupuy, Ron and Prakash 2014; Hossain *et al.* 2017, 2019). Although research on closing **offline** civic space is beginning to receive the attention that it deserves (PartnersGlobal *et al.* 2017; Hossain *et al.* 2018), there has been much less research attention on the openings and closings of **online** civic space in Africa.

When citizens open online civic space, governments often act to close it down. For example, since citizens used SMS (short message service) text messages to organise politically in Tunisia and Egypt in 2011, governments in 50 African countries imposed compulsory SIM (subscriber identity module) card registration (Privacy International 2019). Then, when citizens used social media to voice opposition, some governments blocked it or introduced price rises to make accessing it unaffordable (Nanfuka 2019). Zeynep Tufekci's book *Twitter and Tear Gas* (Tufekci 2017) is a comprehensive account of how citizen use of digital tools in Egypt was met with concerted state repression to close democratic space. Tech-savvy activists initially gained an advantage over established political actors by using mobile and internet campaigning to create online civic spaces. However, governments are now rapidly building their own capabilities to dominate these online spaces using digital surveillance, disinformation and intentional internet disruptions including shutdowns, bandwidth throttling (slowing down), bans and blocking (CIPESA 2016; Freyburg and Garbe 2018; Freedom House 2018; Taye 2020).

Use of online civic space has its own limitations and risks. The ability to access and make productive use of digital technologies is uneven across gender, income, and ethnic groups, such that its patterns of use reflect, reproduce, and amplify existing intersectional inequalities (Hernandez and Roberts 2018; Roberts and Hernandez 2019). Women activists and politicians often face sustained abuse and violence if they are vocal online, creating a chilling effect (Faith and Fraser 2018). The use of mobile devices and online spaces involves leaving digital traces that enable systematic surveillance (Bradshaw and Howard 2019; Zuboff 2019). This digital surveillance is used to target covert voter disinformation and manipulation (Nyabola 2018; Howard 2020); to disrupt internet access to information and communications (Taye 2018); and to mark individuals for arrest, torture or even murder (Ibrahim 2020).

The repressive use of digital technologies by states and corporations has been characterised as 'digital authoritarianism' (Freedom House 2018). The Egyptian and Zimbabwean governments are among those who are known to have imported artificial intelligence-based surveillance technologies from the US and China to spy on their own citizens' mobile and internet communications (Feldstein 2019). Governments are buying new mobile phone interception (Marczak *et al.* 2020) and internet shutdown and disruption technologies (Taye 2020). Politicians are using digital technologies to inflame ethnic division and drown out democratic dialogue and debate (Nyabola 2018; Woolley and Howard 2019). This closes civic space and diminishes citizens' rights to freedom of opinion and expression.

These tactics could threaten the integrity of elections in over 50 African countries that have elections scheduled in the next five years (EISA 2020). They could also influence the outcomes of critical policy debates, including those on vaccines, climate change, gender, and sexual rights – all of which are known targets for digital disinformation and covert influence by powerful foreign and domestic lobbying interests (Jones 2019; Woolley and Howard 2019). In the 2017 elections in Kenya, political elites reportedly spent US$20m on fake news and covert disinformation campaigns designed to manipulate citizens' beliefs and voting behaviour (Brown 2019). In 2020, the number of intentional internet shutdowns by African governments rose from 21 to 25. They were often scheduled at the time of elections or popular protests (Taye 2020). Shutting down the internet reduces the rights to access information and to communicate freely, and the economic right of online traders to conduct business (Statista 2020).

Existing research on the use of digital tools to close civic space is limited, ad hoc, and fragmented. Currently, we know more about digital openings of civic space than we do about digital closings of civic space. We also know far more about the global North than we do about the distinctive features in the global South. The research evidence about African countries that does exist is typically about a single event, or single technology, in a single country. Technical studies are often divorced from consideration of explanatory political and civic contexts. There is currently little comparative analysis on openings and closings of civic space across Africa. Without more detailed empirical evidence about the dimensions and distinctive dynamics of the problem on the African continent, it is impossible for local actors to design effective remedies and countermeasures to restore civic space and secure digital rights.

The ten country reports contained in this collection were commissioned to address these gaps. The reports are from Zimbabwe, Zambia, Uganda, Sudan, South Africa, Nigeria, Kenya, Ethiopia, Egypt, and Cameroon. They are intended to provide an initial scoping of the digital rights landscape within each nation and across the African continent. Each report begins with three sections that review key developments between 2000 and 2020 in the country's political history, civic space dynamics and key technological changes. To aid cross-country comparison, each report contains two summary tables illustrating the timeline of key developments in the opening and closing of civic space, and the use of digital technologies by citizens and governments. The reports present preliminary findings and make tentative recommendations about how to open civic space and enhance citizens' ability to exercise, defend and expand their digital rights.

Initial research results include 180 examples of the use of digital technologies to either open or close civic space. The reports illustrate how wider political dynamics, and increasing availability of mobile and internet technologies, have shaped both openings and closings of civic space. In many of the country reports, the opening of civic space that characterised the years preceding the millennium has been replaced by closing civic space a decade later. The reports provide almost twice as many examples of digital technologies being used to close civic space as to open it. The current wave of surveillance and disinformation technologies has potentially serious implications for the possibility of inclusive dialogue and sustainable development. This **turn to digital authoritarianism** became especially pronounced in the wake of the so-called 'Arab Spring' in 2011, when citizen uprisings unsettled entrenched political elites, who then scrambled to build their own arsenal of digital tactics and techniques to control online discourse.

The country reports show clearly that a comprehensive understanding of digital rights requires cognisance of the wider political, civic space and technological contexts. Taken together, the reports identify the need for an applied research programme that addresses existing gaps in evidence, awareness, legislation, and capacity. We argue that a multi-sector network is necessary to enhance the domestic capacity in each African country to overcome closing civic space and breaches of digital rights. To this end, we recommend engaging with four key constituencies:

- **Researchers** – to produce new **evidence** about surveillance actors, tools, tactics and techniques.
- **Journalists** – to raise **public awareness** about the practices and consequences of surveillance.
- **Policymakers** – to map existing **legislation**, identify gaps and advance a public policy agenda.
- **Activists** – to expand **civic engagement** to tackle surveillance, disinformation and shutdowns.

The next section of this report will outline the literature review that provided the conceptual framing for the ten country reports. Preliminary findings from the country reports are then presented on the range of technologies tools, tactics and techniques identified, before drawing some tentative conclusions and summarising the recommendations made by the report's authors.

2. Literature review

This section presents the literature review and conceptual framing used in commissioning the ten digital rights landscape country reports. The section summarises the literature on: (a) digital rights; (b) civic space and sustainable development; and (c) closing civic space. It concludes by identifying gaps in the existing literature and opportunities for further research.

Human rights are the rights and freedoms that every person is entitled to. The Universal Declaration of Human Rights bestows the same rights on every human irrespective of age, gender, ethnicity, sexuality, wealth, political or religious opinion or other status (UN 1948). These human rights include freedom of opinion and speech, political affiliation, privacy, and assembly. Everyone has the right to information, freedom of association, communication, and direct and indirect participation in political and public affairs (OHCHR 2020).

Digital rights are those same rights in online spaces. Given the increasing centrality of the internet as a space for information exchange and following the findings of the United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression (UNHRC 2011), the UN declared that 'the same rights people have offline must also be protected online'. The UN General Assembly later recognised the 'unique and transformative nature of the internet, not only to enable individuals to exercise their right to freedom of opinion and expression, but also a range of other human rights, and to promote the development of society as a whole' (UNHRC 2018). The African Declaration on Internet Rights and Freedoms (African Declaration 2019) built upon these foundations to provide a detailed articulation of digital rights. The declaration includes a civil society section giving them the duty to 'advocate for Internet rights and freedoms; monitor Internet laws and regulations; and highlight abuses' (*ibid.*).

There is broad agreement that use of digital technologies can enable sustainable development (UNDP 2015; World Bank 2016; WSIS 2018); affect government transparency and accountability (OECD 2018; McGee *et al.* 2018); enhance civil society (Michelson 2006); and play a positive role in women's empowerment (Buskens and Webb 2009; Moolman, Primo and Shackleton 2011; Hafkin 2012; Buskens and Webb 2014). As a result, SDGs include specific targets for extending mobile and internet use (SDG 9c); expanding access to information and communication technologies (ICTs) (SDG 17.6 and 17.8); and women's empowerment (SDG 5b). There is extensive literature documenting the ways in which the use of digital technologies can support social mobilisation and collective action by connecting citizens,

©2021 Tony Roberts & Abrar Mohamed Ali ©Institute of Development Studies. DOI: 10.19088/IDS.2021.005

creating new spaces for engagement between citizens and the state, and helping to empower citizens and strengthen their agency for engagement (McGee *et al.* 2018).

However, the use of digital technologies can also constrain citizens' voices, undermine and obstruct accountability, and facilitate surveillance and repression (*ibid.*). Any technology has more than one potential application. It is common for technologies to be appropriated for purposes other than those originally in the mind of their inventors. As Kranzberg's first law of technology notes, the technologies themselves are neither good nor bad, but nor are they ever neutral (Kranzberg 1986). The inherent 'interpretive flexibility' of technologies (Pinch and Bijker 1984) allows them to be used in 'good' or 'bad' ways, with the use of technologies often reflecting the politics and values of society and users (MacKensie and Wajcman 1985; Feenberg 1992).

Affordances are a useful concept for analysing the use of technology to open and close civic space. The concept of affordances concerns what 'action possibilities' a particular technology allows, invites or enables (Gibson 1977; Norman 1988). For example, the use of social media affords citizens the action possibility of publishing opinion and images instantly, at scale and internationally, enabling real-time reporting of police brutality or viral hashtag campaigns such as #BlackLivesMatter or #MeToo. However, social media also affords governments and corporations the action possibility of surveillance-profiling and disinformation micro-targeting in order to covertly manipulate citizens' beliefs and voting behaviour (O'Neil 2016; Benjamin 2019; Zuboff 2019; Sadowski 2020). Analysing the affordances of different technologies is advantageous in understanding their use in opening and closing civic space in ways that enhance or diminish digital rights.

Africa has experienced a rapid – but uneven – expansion in the use of mobile and internet technologies. This has produced digital dividends for some in the form of improved social and economic development (Buskens and Webb 2014; WSIS 2018). However, access to digital devices and connectivity is uneven, creating new exclusions, and digital divides. These divides exist both within and between countries (World Bank 2016). The use of digital technologies has been shown to reflect, reproduce, and amplify existing patterns of (dis)advantage (O'Neil 2016; Eubanks 2017; Hernandez and Roberts 2018). Technology access and the ability to make effective use of it, is uneven across intersecting divides of gender, class, and ethnicity (Eubanks 2017; Noble 2018; Benjamin 2019). A mobile gender gap exists across low- and middle-income countries: 300 million fewer women than men have access to mobile internet (GSMA 2020). The gap continues to grow between those who are able to regularly upgrade to the latest devices and fastest connections, and those who remain unconnected or digitally illiterate (Roberts and Hernandez 2019).

Uneven digital access and digital literacy create hierarchies of digital citizenship. Citizenship is often understood narrowly as the relationship of rights and responsibilities between an individual and the state. A broader and more inclusive understanding of citizenship focuses on the actions of a person or persons, whether formally documented citizens or not, in exercising, defending, or claiming rights. This agency-based rights-claiming conception of citizenship is the most appropriate in the context of digital rights. **Digital citizenship** is this same rights-claiming citizen agency but in online spaces (Isin and Ruppert 2015; Hintz, Dencik and Wahl-Jorgensen 2019). Due to uneven technology access, not all citizens are digital citizens; and not all digital citizens have equal access to the kind of digital devices, online spaces, or digital literacy necessary to exercise, defend, or expand digital rights.

The UN is among those arguing that an open and vibrant civic space is essential to inclusive democracy and sustainable development (UNDP 2015; World Bank 2016). To reflect this belief SDG 16 commits signatory governments to achieving 'inclusive, participatory, and representative decision-making at every level'; and SDG 17 requires building a partnership for development between civil society, governments, and the private sector (UNDP 2015). All ten countries included in this study are signatories to the SDGs. The UN High-Level Forum on Aid Effectiveness and the High-Level Panel on the 2030 Sustainable Development agenda both underscored the central role of civil society as partners in delivering the SDGs (UN 2013; ACT Alliance and CIDSE 2014; ICNL 2016).

However, in many countries the civic space necessary for inclusive, participatory dialogue and policy deliberation is rapidly shrinking (Dupuy, Ron and Prakash 2016; Hossain *et al.* 2018; CIPESA 2019; Freedom House 2019a). In 2020, over 90 per cent of African countries were experiencing significant restrictions to basic civic freedoms, with only 2 out of 54 countries categorised as having open[3] civic space (CIVICUS 2020). Mechanisms used to close civic space have included deregistering non-governmental organisations, regulations to cut off funding, violence and harassment, arbitrary arrest and disappearance of civil society actors (Dupuy *et al.* 2016; Hossain *et al.* 2018). Citizens who propose policy alternatives, publicly criticise the government or organise political opposition are at risk of arrest and violence (CIVICUS 2019). In terms of political rights and civil liberties, 2020 was the 14th consecutive year of global decline (Freedom House 2020). Trust in politicians and the democratic process is in decline globally (Bertsou 2019). Unless this democratic backsliding is reversed, the global challenge of achieving inclusive and sustainable development as defined in the SDGs is unattainable by 2030.

[3] **CIVICUS Monitor** uses five categories of open, narrowed, obstructed, restricted and closed.

During periods of *closing civic space* activists forced underground or into exile have often fought back by *opening online civic space* from where their right to freedom of speech and assembly can be exercised and defended (Buyse 2018; Roberts 2019). The use of SMS text messages by Kenyan activists to create an online map of unfolding election violence in 2007 (Okolloh 2009; Roberts and Marchais 2018) and by Egyptian feminists to map sexual harassment in Cairo (Peuchaud 2014) are positive examples of using digital technologies to create online civic space. The opening of civic space online has been characterised by hashtag campaigns, viral memes, and civic technologies as mechanisms for digital rights advocacy (Nyabola 2018; Solomon 2018). Online civic space has been particularly valuable for repressed groups to discuss sensitive subjects; to project the voices of underrepresented groups, such as LGBTQI and ethnic minorities; and to propose policies that have been inadequately represented by establishment media and political parties (Tufekci 2017; Gurumurthy, Bharthur and Chami 2017; Hossain *et al.* 2019). However, online civic space is not open to everyone equally. For example, women, including female politicians, and LGBTQI groups often experience gender-based violence in online spaces (APC 2018; Faith and Fraser 2018; Vlahakis 2018).

Repressive governments often deploy digital technologies to *close online civic space*. In recent years, those with political and economic power have been able to expand their arsenal of digital technology tools and tactics to disrupt, drown out or shut down online civic space. This was exemplified by 'political marketing' consultancy Cambridge Analytica testing its covert voter manipulation methods in Kenya's 2013 election prior to their deployment in the UK's Brexit referendum and Donald Trump's 2016 presidential campaign victory (Nyabola 2018; Solomon 2018). In South Africa, another political marketing consultancy, Bell Pottinger, coordinated a network of trolls and bots[4] to fan the flames of racial division for political advantage (Fraser 2017). Political parties now routinely hire private companies – such as Cambridge Analytica and Bell Pottinger – to profile citizens using Facebook, mobile phone and other personal data (Zuboff 2018; Sadowski 2020) in order to micro-target voters with fake news and disinformation, via troll farms, cyborg networks, bot armies,[5] and other 'coordinated inauthentic behaviour' (Bradshaw and Howard 2017; Woolley and Howard 2017; Howard 2020).

Internet surveillance and mobile intercept technologies are now regularly employed by African governments. In addition to the social media surveillance discussed above, African governments are now buying mass surveillance technologies from the US or China to spy on citizens' email

[4] Disinformation can be posted manually by people (called trolls) or automatically by programs (called bots).

[5] Coordinated disinformation campaigns can be run by teams of trolls (working in troll 'farms'), by large numbers of automated bots (called 'bot-nets' or bot armies) and by integrated part-troll-part-bot 'cyborg networks'.

and internet communications (Feldstein 2019; Freedom House 2019). Some African governments are buying new mobile phone interception technologies (Marczak *et al.* 2020), and internet shutdown and disruption technologies (Access Now 2020). The number of intentional internet shutdowns in Africa rose from 21 in 2019 to 25 in 2020 (Taye 2020). In African elections over the next few years, incumbents and powerful challengers will continue to be able to hire troll farms and bot armies to disrupt debate, manufacture opinion and covertly manipulate voting behaviour (Baker and Blaagaard 2016; Bradshaw and Howard 2017; Woolley and Howard 2019). These covert measures damage democracy and diminish digital rights, making impossible the kind of inclusive and participatory governance outlined in the SDGs.

Existing surveillance and disinformation literature is limited in detailing the dimensions and dynamics of the African experience. From the first use of SMS in protest movements (Ekine 2010) to viral social media hashtag campaigns, researchers have documented African citizens' use of mobile phones and social media to open new online spaces (Nyamnjoh 2016; Tufekci 2017; Egbunike 2018). Members of the African Digital Rights Network have made important contributions to the growing literature on the use of digital technologies by citizens to open civic space (Gagliardone 2014; Nyabola 2018; Ojebode 2018; Bosch 2019; Karekwaivanane 2019a; Oosterom 2019; Roberts 2019; CIPESA 2019b, 2020). However, the closing of online civic space by African governments is relatively under-researched. The existing literature on digital surveillance and disinformation is predominantly focused on the global North. Relatively little is known about how these digital practices affect the 1.3 billion citizens of the 54 countries on the African continent. Addressing this gap is urgent given the critical importance of digital rights and open civic space to inclusive democracy and sustainable development. The research that does exist on Africa is primarily composed of single-technology, single-event, and single-country studies. **There is not yet any comparative African literature to identify trends, build theory, and guide policy and practice. Without clear definition of the detail, dimensions, and dynamics of the use of digital technologies to close civic space, it is impossible to design adequate remedies.**

Drawing on this literature review, the African Digital Rights Network resolved to make a preliminary contribution to addressing gaps in existing literature by producing a series of ten digital rights landscape country reports. Our intention was to conduct an initial scoping of which actors are using which digital technologies to both open and close civic space. The concepts of digital rights and literature on closing civic space were central to the framing of the reports. Although the concepts of digital citizenship, gender inequalities, and digital affordances emerged from the literature review as a potentially useful lens, it was decided not to use them to frame the preliminary country reports, and to use them instead in the thematic papers planned in the next research phase.

Country report authors were required to preface their analysis of the digital rights landscape with three sections charting the most relevant political, civic space, and technology developments in each country's history between 2000 and 2020. This was in order to assess the extent to which contextual political events and technology developments affect openings and closings of civic space, and the ability of citizens to exercise their digital rights.

Before presenting the initial findings arising out of the ten digital rights landscape country reports, the next section briefly explains the methodological design and country sample.

3. Methodology

The African Digital Rights Network[6] was established in May 2020 using a Global Challenges Research Fund-UK Research and Innovation Digital Innovation for Development in Africa Networking Grant[7] to develop a network of activists, researchers, journalists, and policymakers working on digital rights in Africa. Its aim was to build new relationships that would stimulate novel research and innovation ideas that enhance citizens' ability to exercise, defend and expand their digital rights.

The network brought together 20 activists, analysts, and academics, some of whom had already published research on the use of digital activism to open civic space (Abraham 2014; Gagliardone 2014; Nyabola 2018; Ojebode 2018; Bosch 2019; Karekwaivanane 2019; Oosterom 2019; Roberts 2019), as well as internet shutdowns and disruption to close civic space (Taye 2019).

The initial focus was to document which actors were using which tools to open and close online civic space; and to identify gaps in evidence, awareness, and domestic capacity. The short-term goal was to inform the articulation of a multi-year research and innovation strategy to enhance digital rights in Africa. In the first six months, network members resolved to conduct an initial scoping of digital rights by producing country reports that provided a preliminary mapping and analysis of the drivers, actors, tools, and tactics being used in the ten countries both to open and close civic space. The medium-term objective was to build capacity for research and innovation that supported change in policy and practice. The longer-term aim was to open civic space and for citizens to be better able to exercise, defend and expand their digital rights.

The authors of ten digital rights landscape reports were asked to identify who was using which digital technologies, tools, tactics, or techniques to either open or close civic space in their country. In order to analyse the drivers of both openings and closings of civic space, authors were asked to preface their analysis of the current digital rights situation with a review of the key political, civic space, and technological developments that have shaped the digital rights landscape since the turn of the millennium. To enable cross-country comparison, each country report adopted this same structure and contained two tables: the first summarised key openings and closings of civic space between 2000 and 2020; while the second provided a timeline of the most relevant digital technology developments for the same period.

[6] **African Digital Rights Network project page**, Institute of Development Studies website.
[7] **GCRF Digital Innovation for Development in Africa**.

The ten-country sample was selected to be representative of the main geographical regions of the continent, as well as a range of levels of civic space openness, political and internet freedoms and economic development (Table 3.1). The sample was also pragmatically shaped by resource constraints, network contacts and positive responses to outreach.

Table 3.1 Country selection

		Freedoms[8]	Civic space[9]	Internet freedom[10]	HDI[11]	Gini coefficient[12]	Internet access (%)[13]
1	**South Africa**	79	Narrowed	70	0.709	63	56.2
2	**Zambia**	54	Obstructed	59	0.584	57	39.3
3	**Kenya**	48	Obstructed	67	0.601	41	87.2
4	**Nigeria**	47	Obstructed	60	0.539	35	61.2
5	**Uganda**	34	Repressed	56	0.544	43	40.5
6	**Zimbabwe**	29	Repressed	46	0.571	44	56.5
7	**Ethiopia**	24	Repressed	29	0.485	35	17.8
8	**Egypt**	21	Closed	26	0.707	32	48.1
9	**Cameroon**	18	Repressed	n/a	0.563	47	29.7
10	**Sudan**	12	Repressed	30	0.510	34	29.9

Note: HDI = Human Development Index

Source: Authors' own.

Rather than produce our own digital rights index, we chose instead to build on existing freedom and civic space scorecards by CIVICUS and Freedom House (see Table 3.1) and contribute country reports that provided a qualitative assessment of the dynamic nature of openings and closings and to document the wide range of digital tools, tactics and techniques being deployed to enhance and constrain digital rights. The intention was that this would enable textured findings that, when analysed, would shed light on the causes and solutions to the diminution of civic space and digital rights.

[8] **Countries and Territories**, Freedom House.
[9] **Monitor: Tracking Civic Space**, CIVICUS.
[10] **Internet Freedom Scores**, Freedom House.
[11] **Human Development Index**, Human Development Reports.
[12] **Gini coefficient index**, World Bank.
[13] **Internet World Stats: Usage and Population Statistics**.

©2021 Tony Roberts & Abrar Mohamed Ali ©Institute of Development Studies. DOI: 10.19088/IDS.2021.005

The ten digital rights country landscape reports were commissioned from network members and external experts. The reports identified 65 examples of digital technologies being used to open civic space across Africa; and 115 examples of technologies, tactics and techniques used to close civic space. Several rounds of inductive coding were used to cluster these examples into ten categories of openings and 12 categories of closings, which are tabulated in the next section.

The country reports were prepared in the second half of 2020 during the coronavirus disease (Covid-19) pandemic. Covid-19 restrictions meant that all research activities had to be desk based and virtual. Research carried out was predominantly qualitative desk review of online secondary sources. The next phase of this research should incorporate primary data collection, including interviews with key informants to validate secondary data sources and deepen analysis in those areas identified as key during this initial scoping (e.g., surveillance, disinformation, and internet shutdowns). This qualitative analysis should be complemented with quantitative data analysis using software such as NodeXL to provide detailed analysis of the dimensions, principal actors and timelines of online hashtag and disinformation campaigns.

The next section presents some preliminary findings from the country reports and discusses their relevance to extending citizens' digital rights.

4. Findings and discussion

When this research was originally conceived, we imagined that our contribution might be to complement the **closing civic space** literature with data and analysis of **opening civic space** online. However, our findings about closing online civic space are at least as significant. Report authors identified almost twice as many examples of digital closings as digital openings.

The ten country reports provide 65 examples of digital openings and 115 examples of digital closings. We categorised the 65 examples of digital technology used to open civic space into ten main categories (Table 4.1). The 115 examples of technologies, tactics and techniques used to close civic space were coded into the 12 categories. The following sections present our findings from a preliminary analysis across the ten country reports and discuss their relevance for opening civic space and enhancing digital rights.

Table 4.1 Digital openings

	Digital openings of civic space – 65 examples presented in 10 categories										
1	Increased – but uneven – access to mobile devices and internet	ZW	ZM	UG	SD	SA	NG	KE	ET	EG	CM
2	SMS activism	ZW	ZM								
3	Social media activism	ZW	ZM	UG	SD	SA	NG	KE	ET	EG	CM
4	Civic tech activism	ZW	ZM			SA	NG	KE	ET		CM
5	Diaspora amplifies message to apply international pressure	ZW		UG	SD		NG	KE	ET		CM
6	Laws conferring new (digital) rights and entitlements		ZM	UG		SA	NG	KE		EG	
7	Digital policies promoting access, rights, open data, etc.					SA	NG	KE			CM
9	Digital security (e.g. Signal, VPNs, encryption)	ZW	ZM		SD					EG	CM
8	Strategic litigation to defend digital rights					SA		KE			
10	IMSI sniffer app	ZW									

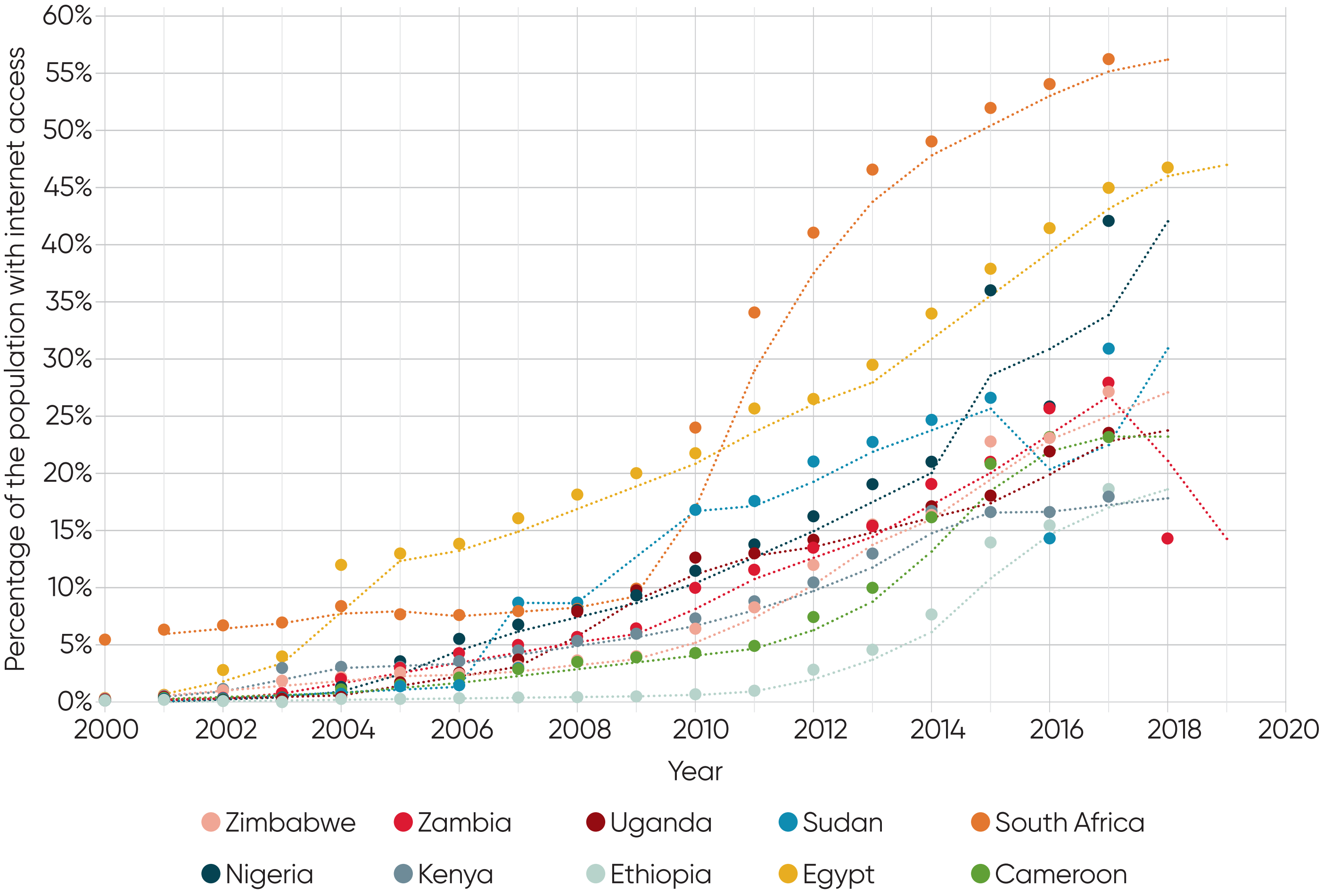
Note: IMSI = International mobile subscriber identity; VPN = virtual private network

Country key: CM = Cameroon; EG = Egypt; ET = Ethiopia; KE = Kenya; NG = Nigeria; SA = South Africa; SD = Sudan; UG = Uganda; ZM = Zambia; ZW = Zimbabwe

Source: Authors' own.

The rapid increase in mobile and internet access is a key driver of opening civic space online. Although computers have long been used by activists, only a small percentage of the population in many countries had access to them. The relatively high levels of mobile phone ownership afforded new action possibilities for wider civic engagement. In all ten country reports the dramatic expansion of mobile phone use and internet access was highlighted as providing new means to instantly exchange information and to communicate interactively over long distances. These new affordances qualitatively increased the speed, scale and reach of citizen-led advocacy and civic engagement. However, as discussed below, access to digital devices and connectivity is uneven across gender and income, such that previously (under)privileged groups are often further (dis)advantaged.

Figure 4.1 Growth in internet access



Source: Adapted from Internet World Stats[14]

[14] **Internet World Stats: Usage and Population Statistics**.

DOI: 10.19088/IDS.2021.005

SMS activism was the first widespread digital tool used to create virtual civic space. The Ethiopia country report (Gagliardone 2021, this collection) shows how the successful use of SMS text messages to issue 'calls to action' during the dramatic opening of civic space ahead of the 2005 election led the government to block and interrupt SMS services. In the country reports on Sudan and Uganda, the authors note that governments became so fearful of the power of SMS after the 2011 uprisings in Tunisia and Egypt that they temporarily blocked SMS in their countries (in this collection: Mohamed Ali 2021 and Nanfuka 2021).

The report by Karekwaivanane (2021, this collection) shows how sending bulk text messages became part of the repertoire of activists' methods in Zimbabwe and resulted in the government issuing a ban on all bulk SMS messaging in 2013. Around the same time, many African governments also started introducing mandatory SIM card registration, taking advantage of the surveillance affordances of mobile phones. Fifty of Africa's 54 countries had mandatory SIM card registration in place by 2019 (Privacy International 2019). Mobile phone SIM card registration removed from citizens the mobile affordance of anonymity, which preserved their right to privacy, and replaced it with the new action possibility for governments to surveil, geolocate, track and target citizens.

Social media activism to open civic space online is the most evident tactic in the ten reports. Although text messaging dominated in the first decade of the millennium, between 2010 and 2020 social media became the most used online civic space. The Zambia and Ethiopia country reports are among those that point to the key role played by independent citizen bloggers in opening online civic space (in this collection: Phiri and Zorro 2021 and Gagliardone 2021). The affordances of social media allowed 'unruly' citizen publication of opinion by individuals from outside establishment media, political parties, or civil society structures (Khanna *et al.* 2013).

However, by the second decade of the millennium corporate social media platforms such as Facebook, Twitter, and WhatsApp had in effect colonised online civic space. Citizens famously made use of Facebook and Twitter in the Egyptian revolution (Farahat 2021, this collection) and the platform quickly became central to digital citizenship across the continent. Some governments that perceive social media as more of a threat than an opportunity have sought to address this threat by blocking or limiting its use. The Zimbabwe government used massive price hikes to make social media unaffordable during periods of civic action, raising the cost by 500 per cent in 2016 and by 2,500 per cent in 2017 (Karekwaivanane 2021, this collection). The Ugandan government introduced a 'social media tax' (Nanfuka 2021, this collection). The majority of country reports (8 out of 10) document incidents in which those using social media to criticise the government are arrested or jailed.

Civic tech activism became a popular way to open civic space in some African countries from around 2010 onwards. The Nigeria country report (Oladapo and Ojebode 2021, this collection) shows how technology activism organisation BudgIT[15] used online space to monitor government budget implementation and hold extractive industries to account. The same report provides the example of activist organisation Enough is Enough Nigeria[16] promoting good governance and citizen engagement using the affordances of digital technologies for connective action (Bennett and Segerberg 2013). The South Africa country report (Bosch and Roberts 2021, this collection) documents the increase in civic tech organisations that afford possibilities for citizen campaigns, civic engagement and budget scrutiny, including Amandla.mobi,[17] GovChat[18] and Vulekamali.[19] Unlike SMS and social media activism, the country reports do not mention government efforts to close down the civic space opened by this form of activism. **Further research could usefully seek to understand whether incumbent governments see civic tech as a significant threat to their interests, whether there are examples of blocking or shutting down civic tech, and whether it is easier to contain and co-opt civic tech**.

Diaspora engagement positively amplifies the international impact of online campaigns. A clear theme emerging from the country reports was the importance of African diaspora engagement in amplifying domestic social media campaigns across the globe. The Cameroon country report (Ndongmo 2021, this collection) provides the example of #AnglophoneCrisis, which went viral internationally. Other hashtag campaigns mentioned in the country reports that were able to enlist the African diaspora to bring international pressure to bear on their governments were the Nigerian #BringBackOurGirls campaign, the Ugandan #FreeStellaNyanzi campaign, and the Ethiopian #FreeZone9Bloggers campaign (in this collection: Oladapo and Ojebode 2021, Nanfuka 2021, and Gagliardone 2021). It is worth noting that the ability for viral citizen-led campaigns to take place is enabled by the digital affordances of social media for instant, global, communication of calls to action, images, and video reportage. **This finding reinforces the need to build international networks of digital rights activists, journalists, and researchers to build public engagement and mobilise political pressure for policy change; and to facilitate South-to-South and international knowledge and experience exchanges**.

[15] **BudgIT**.
[16] **Enough is Enough Nigeria**.
[17] **Amandla.mobi**.
[18] **GovChat**.
[19] **Vulekamali**.

Digital security tools are effective but under-used. A second important theme emerging from the reports was that secure digital practices are useful in opening civic space and extending digital rights. When the Sudanese government in 2018 shut down social media during pro-democracy protests, citizens used virtual private networks (VPNs) to stay online (Mohamed Ali 2021, this collection), but not everyone had the technical awareness to do so. The increase in surveillance and arrests for online speech creates a need for new tools, awareness, and skills to practice online safety and data safeguarding. The use of VPNs helps citizens to disguise their location and evade state censorship and blocking. Digital encryption allows activists and researchers to encode their emails, text and instant messages, and secure sensitive or personal data on their phones or other digital devices.

The uptake of the secure Signal messaging app among activists and journalists is one example of this trend. The Egypt country report notes that its use was considered significant enough for the government to block all use of the Signal app for a week in December 2016 (Farahat 2021, this collection). Too few African citizens, rights activists, and researchers know how to safely save, access, or send sensitive information using mobile phones, email, or apps (THRDC 2016). A significant amount of work has gone into producing digital security toolkits and training (Ganesh and Gutermuth 2014). However, levels of awareness and uptake remain low, and there is no existing knowledge infrastructure to efficiently share new surveillance and security resources. **Work to increase knowledge, make available, and enable effective use of digital security tools like VPNs, Signal and the Tor[20] internet browser should be built into project awareness-raising and capacity-building programmes.**

Intersectional inequalities affect access to civic space, digital citizenship, and digital rights. An emerging theme from the country reports that demands more focused attention in subsequent research phases is the complex ways in which gender and intersectional inequalities shape digital access, digital citizenship, and digital rights (Ganesh, Deutch and Schulte 2016). The country report on Cameroon (Ndongmo 2021, this collection) illustrates how LGBTQI citizens are restricted in their use of physical and online civic space. Similar closing of civic space occurred for citizens in Uganda and Nigeria (in this collection: Nanfuka 2021 and Oladapo and Ojebode 2021).

Civic space and digital rights are sometimes treated as universal categories, but as several country reports in this collection illustrate, women – especially low-income women, black women politicians, and LGBTQI citizens – do not enjoy equal access to digital tools or connectivity. They are subject to gender-based violence online, and this restricts their effective access and rights (APC

[20] Unlike market-leading browsers from Google or Microsoft, the Tor browser disables tracking and cookies.

2018; Faith and Fraser 2018; Vlahakis 2018). It is important to be mindful that the use of all digital technologies generally excludes some entirely, and for others it creates hierarchies of access and ability (Roberts and Hernandez 2019). **In order to produce a more nuanced analysis, subsequent phases of this research should avoid binary conceptions of open/closed civic space and ask, 'Open to whom?' and 'Which civic space?' to produce more detailed and actionable analysis.**

Table 4.3 Digital closings

	Digital closings of civic space – 115 examples presented in 12 categories										
1	Surveillance	ZW	ZM	UG	SD	SA	NG	KE	ET	EG	CM
2	Disinformation	ZW	ZM		SD	SA	NG	KE		EG	
3	Internet shutdowns	ZW	ZM	UG	SD		NG		ET	EG	CM
4	Laws and regulations	ZW	ZM	UG	SD	SA	NG	KE	ET	EG	CM
5	Arrests for online speech	ZW	ZM	UG	SD		NG	KE	ET	EG	CM
6	Closing civic space to specific groups	ZW		UG		SA	NG		ET	EG	CM
7	Mandatory mobile SIM card registration[21]	ZW	ZM	UG	SD	SA	NG	KE	ET	EG	CM
8	Price hikes, social media tax	ZW	ZM	UG							CM
9	Mandatory registration of bloggers		ZM	UG							
10	Mandatory ID for internet cafe use									EG	
11	Bulk SMS ban	ZW									
12	Murder of digital election official							KE			

Country key: CM = Cameroon; EG = Egypt; ET = Ethiopia; KE = Kenya; NG = Nigeria; SA = South Africa; SD = Sudan; UG = Uganda; ZM = Zambia; ZW = Zimbabwe

Source: Authors' own.

Surveillance is the technique mentioned most often in country reports as closing civic space and diminishing digital rights. The Kenya country report documents funding from the US and China to build mass surveillance infrastructure (Nyabola 2018). China and the US supply surveillance technologies to many African countries including Nigeria, South Africa,

[21] Six of the country reports explicitly mention mandatory SIM card registration. We were able to establish that it is compulsory in all ten countries in this study, and in 50 of Africa's 54 countries overall (Privacy International 2019).

Sudan, Egypt, Cameroon, and Zambia. The Government of Uganda is among those which have procured mobile phone intercept technologies from Italian company Hacking Team (Nanfuka 2021, this collection), which also supplies the Sudanese government (Mohamed Ali 2021, this collection). While still in office President Robert Mugabe of Zimbabwe received a 'gift' of monitoring and surveillance technology from Iran that included mobile phone scanners, enabling his government to intercept citizens' private mobile communications and locations (Karekwaivanane 2021, this collection).

In addition to the above state surveillance technologies, the advent of 'surveillance capitalism' (Zuboff 2018) means that African governments are now able to buy surveillance as a commercial service from social media companies, intermediate data brokers, and political marketing consultancies such as Cambridge Analytica and Bell Pottinger. US corporations including Facebook, Twitter, YouTube, and WhatsApp have effectively privatised and monopolised online civic space. This enables those corporations to monitor and track millions of citizens in key marginal constituencies; ascertain their political preferences, 'likes' and trigger issues; predict their voting behaviour; and then sell their digital profiles as a commodity to powerful politicians for targeting and covert manipulation (Bradshaw and Howard 2017; Zuboff 2019; Sadowski 2020). **Minimal detailed research and analysis exists on surveillance drivers, actors, mechanisms, and appropriate responses in Africa. This is a critical area in which further research is urgently needed.**

Surveillance involves an inherent power imbalance between the watcher and the watched. Ways to redress the power imbalance include building public awareness about rights and surveillance practices and building the 'sousveillance' (Mann *et al.* 2003) capacity – or 'inverse surveillance' capacity – of those being watched to better understand the tools and techniques of the watchers and inform the design of effective legal and policy responses. **This inversion of surveillance can be used as a tactic to build the knowledge, agency and critical digital literacy of citizens and to inform policy changes that protect and extend digital rights.**

Disinformation is increasingly common across Africa and a key feature of election campaigns. Disinformation has long been part of political campaigning, but in the era of traditional mass media a single message was broadcast nationwide. Now, increased use of mobile phones and social media affords the possibility to precisely profile millions of citizens and to micro-target each one with highly tailored disinformation messaging, instantly, repeatedly and at relatively low cost. The country reports on Kenya and South Africa are among those that record the use of voter manipulation and political disinformation (in this collection: Nyabola 2021 and Bosch and Roberts 2021).

The affordances of algorithmic analysis and machine learning make this digital disinformation qualitatively and quantitatively distinct from predigital mechanisms. Disinformation is not only used to covertly manipulate citizens' beliefs and voting behaviour, but also to manipulate public opinion on crucial policy issues such as vaccines, climate change, immigration, agriculture and education. The country reports on Sudan and Zimbabwe document disinformation being deployed around the Covid-19 pandemic (in this collection: Mohamed Ali 2021 and Karekwaivanane 2021). The country reports on Cameroon, Kenya and South Africa document the weaponisation of disinformation to enflame ethnic hatred for political gain (in this collection: Ndongmo 2021, Nyabola 2021, and Bosch and Roberts 2021).

Digital disinformation and the use of automated 'computational propaganda' is on the rise in a growing list of countries in Africa (Bradshaw and Howard 2019). There is good reason to expect elections and public policy debates in Africa to continue to be impacted by digital surveillance, profiling and micro-targeting of citizens with disinformation. Disinformation threatens all democracies, but the threat is arguably greatest in fragile democracies: those with weak legal and regulatory oversight, poor institutional protections and where levels of disinformation literacy are lowest. **The clear threat to African democracies, open civic space and digital rights presented by the increasing use of covert disinformation to manipulate citizens' beliefs and behaviour, coupled with significant gaps in our knowledge of the dimensions and dynamics of disinformation in African countries, mean that further research is urgently needed in this area.**

Internet shutdowns are on the rise in African countries. The Ugandan government began blocking individual websites as early as 2006 (Nanfuka 2021, this collection). Now, it is increasingly common for governments to shut down the entire internet or mobile phone system. The number of intentional internet shutdowns by governments in Africa rose to 25 in 2020, up from 21 in 2019, with Algeria, Ethiopia and Sudan the worst-affected countries in Africa (Taye 2020). However, digital disruptions short of nationwide blackouts – such as bandwidth throttling and blocking individual applications, locations, or users – are often not captured in this top-level data and require further research attention. The Sudan country report documents the government's blocking, controlling, jamming, and throttling of pro-democracy websites and private accounts (Mohamed Ali 2021, this collection). The Zambia country report documents the government's 2016 blocking of accountability websites such as Zambian Watchdog (Phiri and Zorro 2021, this collection). **Building domestic capacity to monitor and report on internet shutdowns and disruptions would help raise awareness, protect civic space, and defend digital rights.**

Arrests for online speech feature in nine of the ten country reports. The right to freedom of speech and freedoms of political opinion, affiliation and association are guaranteed in the Universal Declaration of Human Rights and many other international treaties and conventions to which all ten countries in this study are signatories. However, as nine of the ten country reports show, criticising the president or government policies on social media can get you arrested in countries including Egypt, Ethiopia, and Nigeria (in this collection: Farahat 2021, Gagliardone 2021, and Oladapo and Ojebode 2021). The affordances of digital technologies to track the geolocation of a citizen who the state wants to arrest is becoming increasingly easy, as individuals leave digital traces whenever they use social media, use mobile money or a credit card, pass a facial recognition camera, or use their mobile phone (Privacy International 2020).

When citizens open civic space online, governments regularly close it down. A pattern emerges from the country reports of the contestation of civic space between citizens and government online. As citizens incorporate new and different digital tools into their repertoire for opening civic space, some governments develop additional tactics and techniques to counter them and close civic space. Citizens' use of SMS for activism has been followed by bans and mandatory registration; citizen bloggers have been arrested and jailed; social media has been privatised; feminist activists online have been attacked by misogynists; ethnic groups have been targeted; Facebook and Twitter have become sites of surveillance and disinformation; and during protests and elections, governments have intentionally shut down or disrupted online civic space (see Table 4.4).

Table 4.4 Openings and responses

Digital opening	Government responses	Example
SMS activism	Blocking accounts	Uganda, Ethiopia
	Banning bulk SMS	Zimbabwe
	Mandatory SIM registration	Zimbabwe, Uganda, Zambia, Cameroon, Nigeria
Political bloggers	Arresting bloggers	Egypt, Ethiopia, Nigeria, Kenya
Platform activism	Blocking access	Zimbabwe, Zambia, Sudan, Egypt, Nigeria
Facebook, Twitter, etc.	Price hikes	Zimbabwe, Zambia
	Social media tax	Uganda
	Arrests for online speech	All countries except South Africa and Kenya
	Internet shutdowns	All countries except South Africa and Kenya
	Disinformation	Zimbabwe, Sudan, Zambia, South Africa
	Coordinating trolls, cyborgs, bots	Zimbabwe, South Africa, Sudan
Encrypted apps (Signal)	Blocking Signal app	Egypt
	Hacking encrypted messages	Sudan, Uganda, Ethiopia

Source: Authors' own.

Legislation was ranked as highly important in both opening and closing civic space. A series of laws are highlighted in country reports that enhance digital rights by providing freedom of information, legal protections against spying and surveillance, or entitlements to internet access and use. The 2005 Access to Information Acts in Sudan and Uganda are examples of legislation to enable digital citizenship and extend digital rights (in this collection: Mohamed Ali 2021 and Nanfuka 2021).

Several country report sections draw attention to laws that significantly diminish digital rights by giving new powers to the state to surveil and intercept citizens' private communications or which criminalise political speech. The 2010 Cybersecurity Act in Cameroon specifically limits freedom of speech online (Ndongmo 2021, this collection) and the 2012 National Intelligence Service Act in Kenya gives the state new powers of citizen surveillance (Nyabola 2021, this collection). Similarly, the Zimbabwe country report uses the example of the Interception of Communications Act, which was introduced in 2006 in response to increasing use of digital platforms to criticise the government (Karekwaivanane 2021, this collection).

It is clear from reading the country reports that legislation is a potentially powerful mechanism for extending digital access, enabling digital citizenship, expanding civic space, and enhancing digital rights. This preliminary scoping study has only scraped the surface of this critically important issue. **This is an area that requires focused and in-depth attention to survey existing legal provisions, breaches, and gaps, and to identify where and why legal provisions translate into effective protections that expand civic space and digital rights.**

The ten country reports make a series of recommendations arising from their analysis of the digital rights landscape, as summarised in Table 4.5. Foremost among the recommendations is the urgent need to dramatically expand evidence, awareness, and capacity around the threats to democracy presented by surveillance, disinformation, and internet shutdowns. Other recommendations include extending the provision of fast and affordable internet to excluded groups, to review and improve legal protections, and raise awareness about available digital security tools.

Table 4.5 Recommendations

	Recommendation	Actors	Countries									
1	Further research and research partnerships	Universities and research institutions	ZW	ZM	UG	SD	SA	NG	KE	ET	EG	CM
2	Capacity-building and strengthening programmes	Civil society	ZW	ZM	UG		SA		KE	ET	EG	
3	Access to fast and affordable internet	Governments			UG	SD	SA				EG	CM
4	Disinformation awareness	Public and journalists	ZW			SD	SA	NG		ET	EG	CM
5	Anti-surveillance awareness (e.g. VPNs, Tor, Signal)	Public and civil society	ZW	ZM	UG	SD			KE		EG	CM
6	Strategic litigation to defend digital rights	Lawyers	ZW		UG		SA				EG	
7	Advocacy for domestic digital rights law	Civil society			UG	SD		NG	KE		EG	
8	South–South networks and knowledge exchanges	CSOs		ZM		SD			KE			
9	Local language translation of digital rights materials	Civil society					SA		KE			

Country key: CM = Cameroon; EG = Egypt; ET = Ethiopia; KE = Kenya; NG = Nigeria; SA = South Africa; SD = Sudan; UG = Uganda; ZM = Zambia; ZW = Zimbabwe

Source: Authors' own.

Building domestic capacity to monitor, analyse and develop solutions to closing civic space is fundamental to improving digital rights. All the country reports identified gaps in knowledge, public awareness, and civil society capabilities. The reports' authors make a series of recommendations designed to mitigate and overcome the threat to democracy posed by growing digital authoritarianism. Local activists, journalists, researchers, and policymakers lack detailed knowledge of the dimensions of digital surveillance, disinformation, and disruption in their countries. The Zambia country report is one of several to recommend that civil society actors should be equipped with the necessary skills and technologies to enable the systematic monitoring of state and private actors' online disinformation

(Phiri and Zorro 2021, this collection). The Zimbabwe country report concludes that there is an urgent need to build domestic technical abilities to monitor, analyse and combat the increased use of surveillance and digital propaganda by pro-government actors (Karekwaivanane 2021, this collection). **Until local actors can accurately detail the dimensions and dynamics of the problem in their own countries, it is impossible for them to define and develop effective countermeasures to restore civic space and digital rights.**

Digital citizenship, digital affordances and digital inequalities are potentially useful conceptual lenses for the future study of civic space and digital rights. Analysing the findings from the ten digital rights landscape country reports has made clear the importance of contextual political, civic space, and technological developments to understand the digital rights landscape in a country. New laws and technical innovations need to be part of opening civic space online to expand digital rights. However, approaches that ignore the wider political dynamics and power imbalances will be insufficient and potentially counterproductive. The conceptual framing of digital citizenship has emerged as a potentially useful means to centre citizen agency and rights-claiming as phenomena that need to be expanded, rather than relying more narrowly on techno- or legal-centric perspectives. Throughout this exercise, the concept of affordances has proved to be a valuable lens for understanding and articulating the possibilities for action afforded by specific technologies for opening or closing civic space and digital rights. We acknowledge that to date we have paid insufficient attention to how different social groups experience unequal access to digital technologies and unequal civic space online in ways that constrain the scope of their digital citizenship and ability to exercise digital rights. In future research it will be important to ask, 'Open to whom?' and 'Open by how much?' in order to produce a more nuanced analysis of who is (dis)advantaged when civic space is opened or closed.

5. Conclusion

The digital rights landscape country reports set out to provide new evidence about the drivers, actors, tools and techniques being used to open and close civic space in ten African countries. We set out to understand more about how digital rights were being shaped by the wider political, civic space and technological landscape. We documented 180 examples that illustrate who is using which digital technologies, in which countries, to either open or close civic space, and with what implications for digital rights.

At the outset, we imagined that our contribution would mainly illustrate the range of creative ways that citizens have responded to closing civic space **offline** by opening civic space **online**. In fact, our contribution is as much about how powerful actors are now **closing** civic space online. We found nearly twice as many examples of the use of digital tactics to close civic space online as we found of the use of digital tactics to open civic space online. A pattern emerged of citizens using digital technologies to open civic space online and exercise their digital rights, and of governments using digital technologies to close civic space online and diminish digital rights.

Although digital technologies are potentially available to anyone, unequal power relationships explain unequal patterns of access and an overall decline in democratic space and digital rights. Some citizens gain access to digital technologies, online civic space, and a degree of digital citizenship. However, governments have access to pervasive digital surveillance, and the ability to deploy disinformation and covertly manipulate citizens' beliefs and behaviour; and they can choose to shut down the internet or imprison citizens for online speech. The country reports also provide examples of civic space being closed by powerful actors **other than governments**, including corporations and dominant gender or ethnic groups, which sometimes also use their power to disrupt democratic dialogue, dominate discourse, and diminish digital rights.

These findings resonate with Kranzberg's first rule that technologies themselves are neither good nor bad, but they are never neutral. Technologies such as social media have affordances that can be used to open civic space, close civic space, or both. How they are used in practice will generally reflect wider political dynamics. Unequal power relationships result in unequal access to technologies; unequal ability to open or close civic space; uneven digital citizenship capabilities and digital rights. The country reports make several key recommendations about how to increase the power of citizens to better exercise, defend and expand their digital rights.

DOI: 10.19088/IDS.2021.005

All ten country reports identify gaps in existing evidence, awareness, and civil society capacity to independently monitor, analyse, and respond to activities that close civic space and diminish digital rights. A key recommendation overall is for further research by African researchers and activists to increase what is known about the dimensions and distinctive dynamics of emerging tactics in digital surveillance and disinformation.

Until local researchers, journalists, activists, and policymakers can accurately detail the dimensions and dynamics of problems in their own countries, it is impossible for them to define and develop effective countermeasures to restore civic space and digital rights. The necessary research should not be conducted in an ivory tower. An applied multi-actor, interdisciplinary research programme is required to build domestic capacity in each country to effectively monitor, analyse and overcome threats to democratic space and digital rights.

While further research, technical capacity and legal remedies are necessary elements of the solution, they are likely to prove insufficient in isolation from raised public awareness and citizen-led political movement for change. Any such movement requires an active alliance of multiple actors and initiatives. As indicated in section 1, the next steps therefore involve working with:

- **Researchers** – to produce new **evidence** about surveillance actors, tools, tactics and techniques.
- **Journalists** – to raise **public awareness** about the practices and consequences of surveillance.
- **Policymakers** – to map existing **legislation**, identify gaps and advance a public policy agenda.
- **Activists** – to expand **civic engagement** to tackle surveillance, disinformation and shutdowns.

References

Abraham, K. (2014) 'Sex, Respect and Freedom from Shame: Zambian Women Create Space for Social Change Through Social Networking', in I. Buskens and A. Webb (eds), *Women and ICT in Africa and the Middle East*, London: Zed Books

ACT Alliance and CIDSE (2015) ***Space for Civil Society: How to Protect and Expand an Enabling Environment***, Switzerland and Brussels: Act Alliance and CIDSE (accessed 26 January 2021)

African Declaration (2019) ***African Declaration on Internet Rights and Freedoms*** (accessed 26 January 2021)

APC (2018) ***Annual Report 2018***, Manila: Association for Progressive Communications (accessed 26 January 2021)

APC (2006) ***APC Internet Rights Charter***, South Africa: Association for Progressive Communications (accessed 26 January 2021)

Assefa, A. and Zewde, B. (2008) *Civil Society at the Crossroads: Challenges and Prospects in Ethiopia*, Addis Ababa: Forum for Social Studies

Baker, M. and Blaagaard, B. (2016) *Citizen Media and Public Spaces*, London: Routledge

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*, New York: Polity Press

Bennett, W. and Segerberg, A. (2013) *The Logic of Connective Action*, Cambridge: Cambridge University Press

Bertsou, E. (2019) 'Rethinking Political Distrust', *European Political Science Review* 11.2: 213–30

Bosch, T. (2019) 'Social Media and Protest Movements in South Africa: #FeesMustFall and #ZumaMustFall', in M. Dwyer and T. Molony (eds), *Social Media and Politics in Africa*, London: Zed Books

Boyd, D. (2010) 'Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications', in Z. Papacharissi (ed.), *Networked Self: Identity, Community, and Culture*, Oxon and New York: Routledge

Bradshaw, S. and Howard, P. (2019) ***The Global Disinformation Order 2019: Global Inventory of Organised Social Media Manipulation***, Working Paper 2019.3, Oxford: Project on Computational Propaganda, University of Oxford (accessed 26 January 2021)

Bradshaw, S. and Howard, P. (2017) ***Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation***, Working Paper 2017.12, Oxford: Project on Computational Propaganda, University of Oxford (accessed 26 January 2021)

Brown, E. (2019) **'Online Fake News is Costing Us $78 billion Globally Each Year'**, ZDNet, 18 December (accessed 26 January 2021)

Buskens, I. and Webb, A. (eds) (2014) *Women and ICT in Africa and the Middle East*, London: Zed Books

Buskens, I. and Webb, A. (eds) (2009) *African Women and ICTs*, London: Zed Books

Buyse, A. (2018) 'Squeezing Civic Space: Restrictions on Civil Society Organizations and the Linkages with Human Rights', *International Journal of Human Rights* 22.8: 966–88

CIPESA (2019a) ***2019 State of Internet Freedom in Africa Report Launched: African Countries are Broadening Control Over the Internet***, Kampala: Collaboration on International ICT Policy in East and Southern Africa (accessed 26 January 2021)

CIPESA (2019b) ***The Shrinking Civic Space in East Africa***, Kampala: Collaboration on International ICT Policy in East and Southern Africa (accessed 26 January 2021)

CIPESA (2016) ***Analysis of Twitter During the 2016 Presidential Debates***, Kampala: Collaboration on International ICT Policy in East and Southern Africa (accessed 26 January 2021)

CIVICUS (2020) ***People Power Under Attack 2020***, Johannesburg: CIVICUS (accessed 26 January 2021)

CIVICUS (2019) ***State of Civil Society Report 2019***, Johannesburg: CIVICUS (accessed 26 January 2021)

Dahir, A. (2018) **'In a Continent Dominated by WhatsApp, Ethiopia Prefers Telegram'**, *Quartz*, 24 February (accessed 20 October 2019)

Dupuy, K.; Ron, J. and Prakash, A. (2016) 'Hands Off My Regime! Governments' Restrictions on Foreign Aid to Non-Governmental Organizations in Poor and Middle-Income Countries', *World Development* 84: 299–311 (accessed 10 February 2021)

Dupuy, K.; Ron, J. and Prakash, A. (2014) '**Who Survived? Ethiopia's Regulatory Crackdown on Foreign-Funded NGOs**', *Review of International Political Economy* 22.2: 419–59, DOI: 10.1080/09692290.2014.903854 (accessed 10 February 2021)

Egbunike, N. (2019) 'Social Media Propelled Ethnocentric Disinformation and Propaganda During the Nigerian Elections', *Global Voices*, 6 November

Egbunike, N. (2018) '**Hashtags: Social Media, Politics and Ethnicity in Nigeria**', *Literary Everything*, 12 November (accessed 26 January 2021)

EISA (2020) ***2021 African Election Calendar,*** Electoral Institute for Sustainable Democracy in Africa (accessed 26 January 2021)

Ekine, S. (ed.) (2010) *SMS Uprising: Mobile Activism in Africa*, Cape Town: Pambazuka Press

Eubanks, V. (2017) *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*, New York: St Martin's Press

Faith, B. and Fraser, E. (2018) *Digital Harassment of Women Leaders: A Review of the Evidence*, VAWG Helpdesk Research Report 209, UK: Department for International Development

Feenberg, A. (1992) '**Subversive Rationalization: Technology, Power, and Democracy**', *Inquiry: An Interdisciplinary Journal of Philosophy* 35: 3–4: 301–22 (accessed 10 February 2021)

Feldstein, S. (2019) ***The Global Expansion of AI Surveillance***, Carnegie Endowment for International Peace (accessed 26 January 2021)

Figari, A.; Diehm, C. and Lawrence, R. (2019) ***Shrinking Civil Space: A Digital Perspective***, Berlin: Tactical Tech (accessed 26 January 2021)

Fraser, A. (2017) '**We Go Inside the Guptabot Fake News Network**', *Tech Central*, 4 September (accessed 26 January 2021)

Freedom House (2020) ***A Leaderless Struggle for Democracy*** (accessed 26 January 2021)

Freedom House (2019) ***The Spread of Anti-NGO Measures in Africa: Freedoms Under Threat*** (accessed 26 January 2021)

Freedom House (2018) ***The Rise of Digital Authoritarianism*** (accessed 26 January 2021)

Freyburg, T. and Garbe, L. (2018) '**Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa**', *International Journal of Communication* 12: 3896–3916 (accessed 26 January 2021)

Gagliardone, I. (2016) *The Politics of Technology in Africa: Communication, Development, and Nation-Building in Ethiopia*, Cambridge: Cambridge University Press

Gagliardone, I. (2014) 'New Media and the Developmental State in Ethiopia', *African Affairs* 113.451: 279–99

Ganesh, M.I. and Gutermuth, L. (2014) ***Case Study: Women's Rights Campaigning: Info-Activism Toolkit***, Tactical Technology Collective (accessed 26 January 2021)

Ganesh, M.I.; Deutch, J. and Schulte, J. (2016) ***Privacy, Anonymity, Visibility: Dilemmas in Tech Use by Marginalised Communities***, Brighton: Institute of Development Studies (accessed 26 January 2021)

Gaventa, J. (2005) *Reflections on the Uses of the Power Cube Approach for Analysing Spaces, Places and Dynamics of Civil Society Participation and Engagement*, CPF Evaluation Series 4: Mfp Breed Netwerk

Gibson, J. (1977) 'The Theory of Affordances', in R. Shaw and J. Bransford (eds), *Perceiving, Acting, and Knowing: Toward and Ecological Psychology*, London: Oxford University Press

GISWatch (2019) *Artificial Intelligence: Human Rights, Social Justice and Development*, Association for Progressive Communications

GISWatch (2014) ***Communications Surveillance in the Digital Age***, Association for Progressive Communications and Hivos (accessed 26 January 2021)

Global Witness (2016) ***On Dangerous Ground***, London: Global Witness (accessed 26 January 2021)

Greene, T. (2019) '**How a Ban on Political Ads is the Second Best Gift Twitter Ever Gave Trump**', TNW, 7 November (accessed 26 January 2021)

GSMA (2020) **The Mobile Gender Gap Report 2020**, London: GSMA (accessed 26 January 2021)

Gurumurthy, A.; Bharthur, D. and Chami, N. (2017) ***Voice or Chatter? Making ICTs Work for Transformative Engagement: Research Report Summary***, Brighton: Institute of Development Studies (accessed 26 January 2021)

Hafkin, N. (2012) 'Gender', in G. Sadowski (ed.), *Accelerating Development Using the Web: Empowering Poor and Marginalized Populations*, London: WebFoundation

Hernandez, K. and Roberts, T. (2018) ***Leaving No One Behind in a Digital World***, K4D Emerging Issues Report 10, Brighton: Institute of Development Studies (accessed 26 January 2021)

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

Hossain, N.; Khurana, N.; Mohmand, S.; Nazneen, S.; Oosterom, M.; Roberts, T. *et al.* (2018) ***What Does Closing Civic Space Mean for Development?*** IDS Working Paper 515, Brighton: Institute of Development Studies (accessed 26 January 2021)

Hossain, N.; Khurana, N.; Nazneen, S.; Oosterom, M.; Schröder, P. and Shankland, A. (2019) *Development Needs Civil Society – The Implications of Civic Space for the SDGs*, Geneva: Act Alliance

Hossain, N.; Khurana, N.; Oosterom, M.; Roberts, T.; Santos, R. and Shankland, A. (2017) 'The Implications of Closing Civic Space for Development', report for DFID, unpublished

Howard, P. (2020) *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*, New Haven CT: Yale University Press

Ibrahim, K. (2020) *Monitored and Targeted: Sale of Surveillance Technology Puts Lives of MENA Activists at Risk*, IFEX

ICNL (2016) '**Survey of Trends Affecting Civic Space: 2015–16**', *Global Trends in NGO Law: A Quarterly Review of NGO Legal Trends around the World* 7.4 (accessed 10 February 2021)

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

Jones, K. (2019) ***Online Disinformation and Political Discourse: Applying a Human Rights Framework***, Research Paper, London: Chatham House, Royal Institute of International Affairs (accessed 10 February 2021)

Jorgensen, R. (2006) *Human Rights in the Global Information Society*, Cambridge MA: MIT Press

Karekwaivanane, G. (2019a) ' "Tapanduka Zvamuchese": Facebook, "Unruly Publics", and Zimbabwean Politics', *Journal of East African Studies* 13.1: 54–71

Karekwaivanane, G. (2019b) 'We Are Not Just Voters, We Are Citizens: Social Media, the #Thisflag Campaign and Insurgent Citizenship in Zimbabwe', in M. Dwyer and T. Molony (eds), *Social Media and Politics in Africa*, London: Zed Books

Khanna, A.; Mani, P.; Patterson, Z.; Pantazidou, M. and Shqera, M. (2013) ***The Changing Faces of Citizen Action: A Mapping Study through an 'Unruly' Lens***, IDS Working Paper 423, Brighton: Institute of Development Studies (accessed 26 January 2021)

Kode, D. (2018) '**Civic Space Restrictions in Africa: How Does Civil Society Respond?**', Conflict Trends 2018.1: 10–17 (accessed 26 January 2021)

Kranzberg, M. (1986) '**Technology and History: "Kranzberg's Laws"**', *Technology and Culture* 27.3: 544–60 (accessed 26 January 2021)

MacKensie, D. and Wajcman, J. (eds) (1985) *The Social Shaping of Technology*, Buckingham: Open University Press

Mann, S.; Nolan, J. and Wellman, B. (2003) 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments', *Surveillance and Society* 1.3: 331–55

©2021 Tony Roberts & Abrar Mohamed Ali ©Institute of Development Studies. DOI: 10.19088/IDS.2021.005

Marczak, B.; Scott-Railton, J.; Rao, S.; Anstis, S. and Deibert, R. (2020) ***Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles***, The Citizen Lab (accessed 26 January 2021)

McGee, R.; Edwards, D.; Anderson, C.; Hudson, H. and Feruglio, F. (2018) ***Appropriating Technology for Accountability: Messages from Making All Voices Count***, Making All Voices Count, Research Report, Brighton: Institute of Development Studies (accessed 26 January 2021)

Michelson, E. (2006) '**Clicking Toward Development: Understanding the Role of ICTs for Civil Society**', *Journal of Technology Studies* 32.1: 53–63 (accessed 26 January 2021)

Moolman, J.; Primo, N. and Shackleton, S-J. (2011) '**Introduction: Taking a Byte of Technology: Women and ICTs**', *Agenda: Empowering Women for Gender Equity* 21.1: 4–14 (accessed 26 January 2021)

Mudhai, O.; Tettey, W. and Banda, F. (2009) *African Media and the Digital Public Sphere*, Hampshire: Palgrave MacMillan

Nanfuka, J. (2019) '**Social Media Tax Cuts Ugandan Internet Users by Five Million, Penetration Down From 47% to 35%**', 31 January, Kampala: Collaboration on International ICT Policy for East and Southern Africa (accessed 26 January 2021)

Noble, S. (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York: New York University Press

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

Nyabola, N. (2018) *Digital Democracy, Analogue Politics: How the Internet Era is Transforming Politics in Kenya (African Arguments)*, London: Zed Books

Nyamnjoh, F. (2016) *#RhodesMustFall: Nibbling at Resilient Colonialism in South Africa*, Bamenda: Langaa RPCIG

O'Neil, C. (2016) *Weapons of Math Destruction*, London: Penguin Random House

OECD (2018) '**Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact**,' *OECD Digital Government Studies*, Paris: Organisation for Economic Co-operation and Development (accessed 26 January 2021)

OHCHR (2020) ***OHCHR and Equal Participation in Political and Public Affairs***, Office of the High Commissioner for Human Rights (accessed 26 January 2021)

Ojebode, A. and Oladapo, W. (2018) '***Using Social Media for Long-Haul Activism: Lessons from the BBOG Movement in Nigeria***', Briefing, Partnership for African Social Governance Research (accessed 26 January 2021)

Okolloh, O. (2009) 'Ushahidi or Testimony: Web 2.0 Tools for Crowdsourcing Crisis Information', *PLA Notes* 59: 65–70

Oosterom, M. (2019) '**The Implications of Closing Civic Space for Sustainable Development in Zimbabwe**', mimeo, IDS and ACT Alliance (accessed 26 January 2021)

PartnersGlobal; Roig, J.; Gomez Chow, L.; Barringer, D. and Vasquez-Yetter, R. (2017) ***The Importance of Ensuring an Enabling Environment for Civil Society as It Relates to the Sustainable Development Goals***, Report to the Working Group on Enabling and Protecting Civil Society of the Community of Democracies, Washington DC: Community of Democracies (accessed 26 January 2021)

Peuchaud, S. (2014) 'Social Media Activism and Egyptians' Use of Social Media to Combat Sexual Violence', *Health Promotion International* 29.suppl 1: i113–i120

Pinch, T. and Bijker, W. (1984) '**The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other**', *Social Studies of Science* 14.3: 399–441 (accessed 26 January 2021)

Privacy International (2019) '**Africa: SIM Card Registration Only Increases Monitoring and Exclusion**', *Privacy International*, 5 August (accessed 26 January 2021)

Roberts, T. (2019) ***Closing Civic Space and Inclusive Development in Ethiopia***, IDS Working Paper 527, Brighton: Institute of Development Studies (accessed 26 January 2021)

Roberts, T. and Hernandez, K. (2019) '**Digital Access is not Binary: The 5 'A's of Technology Access in the Philippines**', *Electronic Journal of Information Systems in Developing Countries* 85.4 (accessed 26 January 2021)

Roberts, T. and Marchais, G. (2018) ***Assessing the Role of Social Media and Digital Technology in Violence Reporting***, IDS Working Paper 492, Brighton: Institute of Development Studies (accessed 26 January 2021)

Sadowski, J. (2020) ***Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World***, Cambridge MA: MIT Press (accessed 26 January 2021)

Solomon, S. (2018) '**Cambridge Analytica Played Roles in Multiple African Elections**', *VOA News*, 22 March (accessed 26 January 2021)

Statista (2020) '**Number of Affected Users and Economic Cost of Internet Shutdowns Worldwide 2019**,' Statista, 25 January (accessed 26 January 2021)

Taye, B. (2020) ***Targeted, Cut Off and Left in the Dark: The #KeepItOn Report on Internet Shutdowns in 2019***, Access Now (accessed 26 January 2021)

Taye, B. (2018) ***The State of Internet Shutdowns Around the World: The 2018 #KeepItOn Report***, Access Now (accessed 26 January 2021)

THRDC (2016) ***Annual Report 2016***, Arusha: Tanzania Human Rights Defenders Coalition (accessed 26 January 2021)

Tufekci, Z. (2017) *Twitter and Tear Gas*, New Haven CT: Yale University Press

UN (2015) *Transforming Our World: The 2030 Agenda for Sustainable Development*, A/RES/70/1, New York: United Nations

UN (2013) ***A New Global Partnership: Eradicate Poverty and Transform Economies Through Sustainable Development: The Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda***, New York: United Nations (accessed 26 January 2021)

UN (1948) ***Universal Declaration of Human Rights***, New York: United Nations (accessed 26 January 2021)

UNDP (2015) *The 2030 Agenda for Sustainable Development*, New York: United Nations Development Programme

UNHRC (2018) ***Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet***, Geneva: United Nations Human Rights Council (accessed 26 January 2021)

UNHRC (2011) ***Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression***, New York: United Nations Human Rights Council (accessed 26 January 2021)

Vlahakis, M. (2018) *Breaking the Silence: Ending Online Violence and Abuse Against Women's Rights Activists*, London: Womankind Worldwide

We Are Social (2019) *Digital 2019: Global Digital Overview*, Hootsuite

Woolley, S. and Howard, P. (2019) *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*, Oxford: Oxford University Press

Woolley, S. and Howard, P. (2017) *Computational Propaganda*, Working Paper 2017.11, Oxford Internet Institute: Project on Computational Propaganda

World Bank (2016) ***World Development Report 2016: Digital Dividends***, Washington DC: World Bank (accessed 26 January 2021)

WSIS (2018) ***Leveraging ICTs to Build Information and Knowledge Societies for Achieving the Sustainable Development Goals (SDGs)***, World Summit on the Information Society (WSIS) Forum 2018 Outcome Document, Geneva: International Telecommunication Union (accessed 26 January 2021)

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, London: Profile Books