Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa

TINA FREYBURG[1]
LISA GARBE
University of St.Gallen, Switzerland

The Internet is often portrayed as offering new communication and information channels resistant to state control because of its decentralization. At the same time, the Internet relies on a hierarchical physical infrastructure that, connecting the individual customer to the Internet, provides states with control opportunities. We argue that ownership of the Internet infrastructure, in particular Internet service providers (ISPs), is critical to understanding state Internet control because most direct forms of control require ISPs to comply with government requests. Using qualitative comparative analysis, we systematically link documented Internet shutdowns in sub-Sahara African countries to configurations of ISP state majority ownership, regime type, and election violence. The results support a positive relationship between a temporary halt of Internet provision and ISP majority ownership by authoritarian states when facing election-related violence. Our study underlines the importance of varying ownership structures in explaining political effects of Internet penetration, including its role in challenging authoritarian rule.

*Keywords***:** *elections, Internet service provision, Internet shutdown, ownership; Sub-Saharan Africa*

"Victory!" the international nonprofit digital-rights advocacy group Access Now exclaimed in August 2016. "President of Ghana says no to Internet shutdowns during coming elections" in December (Olukotun, 2016). Such were the times that even Africa's most stable democracies considered intentionally restricting public Internet access during election periods. In 2015–6, in half of the sub-Sahara African (SSA) countries in which presidential or parliamentary national elections were held, the

Tina Freyburg: tina.freyburg@unisg.ch
Lisa Garbe: lisa.garbe@unisg.ch
Date submitted: 2017–12–07

[1] Financial support by the Swiss Network for International Studies (SNIS) is gratefully acknowledged. We wish to thank Véronique Wavre for her excellent collaboration as well as Marlies Glasius, Marcus Michaelsen, and the three reviewers for valuable input. The Online Appendix can be downloaded from my website (http://www.tina-freyburg.eu/1/135/resources/publication_2903_1.pdf).

government ordered Internet shutdowns as voters headed to polling stations. When in Gambia citizens were called to vote for a president in 2016, access to mobile Internet and text messaging was completely cut off on the polling day and had already been hampered during the electoral campaign. News reporting in the media and various digital rights blogs suggest a positive relationship between elections and shutdowns of Internet services in electoral authoritarian regimes (Odhiambo, 2017). Here, incumbents are commonly said to justify these politically motivated interruptions by citing national security concerns and fears of the spread of fake election results. Commentators agree, however, that this brute-force method of cutting all access is predominantly meant to prevent opponents from organizing protests or reporting election malfeasance.

Although shutting down the Internet during polls is a popular tool of African rulers, the temporary interruption of the flow of digital-based information and communication is no default option. Overall, it appears that democratic rulers refrain from interrupting the flow of digital information during election times. When it comes to Africa's autocracies, however, the picture appears mixed. Uganda, Burundi, Ethiopia, Chad, and the Republic of Congo interrupted access to the Internet during election times. In the Central African Republic (CAR), in turn, in which instability and sectarian violence marked the electoral chaos in 2015–6, digital communication and information continued to flow over the whole lengthy electoral period ("Central African Republic," 2016). The observer might add that the parliamentary and presidential elections as such took place peacefully in CAR; hence, the incumbent might have felt less pressure to block access. The absence of electoral conflict alone, however, appears insufficient to explain cases in which we see no shutdown of Internet services in times of authoritarian elections. The 2015 Togolese presidential elections, for instance, took place without major incidents, but the incumbent president Gnassingbé still experimented with disrupting the Internet.

In this article, we argue that ownership of the physical Internet infrastructure, in particular Internet service providers (ISPs), is key when it comes to explaining incidences of Internet shutdowns. Governments typically do not directly restrict Internet access but order telecom operators and other autonomous systems (ASs) that provide Internet to halt their services. Because ISPs provide "last-mile" connection to end users, governments rely on their cooperation if they intend to cut access to particular services or entire (sub-) networks. Yet existing political science scholarship largely views the Internet not only as a technical "black box" but also as a resource that governments have at their free disposal. It hence tends to treat the structure of ISP ownership as a constant rather than a variable.

We, in contrast, view Internet services as a good, owned by different private and public actors with potentially diverging interests, and consider the complex physical infrastructure essential for its provision. Few studies have identified varying ownership arrangements as crucial for the economic and political consequences of Internet penetration (on corruption and growth, e.g., Dasgupta, Lall, & Wheeler, 2005; on state repression, e.g., Milner, 2006; Pallin, 2017). Given that most of these studies focus only on specific countries and short time periods, or exclusively rely on descriptive assessments, the findings produced can be seen as limited in their power both to explain and to generalize. Consequently, the relationship between ownership and political outcomes of Internet service provision, including its temporary interruption at times of political contestation, has largely been ignored.

Although a few studies suggest that strategies of political repression such as censorship and (situational) disruption are implemented more effectively if the government is able to control the infrastructure (Weber, 2011), the role of telecom companies, in particular, private intermediaries in enabling or disabling network disruptions, has not yet been systematically explored (Corrales & Westhoff, 2006; Weidmann, 2015). Drawing on insights from studies of the political effects of varying ownership over natural resources (Luong & Weinthal, 2006; Wegenast & Schneider, 2017) and media (Stockmann, 2013), and borrowing the concept of technopolitics from the history of technology tradition (Hecht, 2001; Hughes, 1983), we expect the occurrence of Internet shutdowns to coincide with specific ISP ownership arrangements. Precisely, we contend that the temporal interruption of Internet services is facilitated if the state is the majority owner of at least one ISP operating on its territory; by the same token, it should be more challenging for a government to make ISPs comply with its request if the majority of ISPs on its territory is in private hands. This relationship should be even more prominent in times of electoral conflict that may be perceived by the incumbent ruler as threatening reelection and hence political survival.

Empirically, we systematically investigate the link between state majority ownership of ISPs in a country and the politically motivated temporal interruption of access to the Internet during contentious events, namely the 33 presidential and parliamentary elections in SSA between 2014 and 2016. To examine whether state majority ownership of ISPs is associated with Internet shutdowns, in particular at times of election violence, we use a novel data set of ISP ownership (Freyburg, Garbe, & Wavre, 2018) that we combine with documented Internet shutdowns (our outcome), plus a binary measure of (nongovernmental) election violence, as compiled by the global Varieties of Democracy (V-DEM) data set (Coppedge et al., 2017), and a dichotomous measure of a country's regime type based on Polity IV (Marshall, Gurr, & Jaggers, 2017).

We focus on SSA because this region of the world is especially marked by economic and political transitions that we expect to drive cross-national variation in ISP ownership. Most of them have recognized investment in ICT as crucial driver of economic growth (Albiman & Sulong, 2016). Privatization has often diversified the market by reducing the traditionally leading role of the state and increasing private-sector involvement. Plus, the third wave of democratization has been particularly prominent in SSA; still, countries show varying degrees of political liberalization (Levitsky & Way, 2010). Democracy is the norm today, albeit imperfect, with most governments coming to power through competitive elections, and most rulers following civilian rather than military careers. Yet the struggle for democracy has not been entirely successful; major reversals still appear frequently throughout the region. And, crucially, Internet shutdowns have become a particularly popular tool, especially for autocracies during times of elections.

In the following, we first conceptualize Internet shutdowns and point to their relevance during election periods. Subsequently, we explain the role of ISPs in disrupting Internet services and why their ownership matters for the (non-)occurrence of shutdowns. We then derive propositions regarding the link between ISP state majority ownership and Internet shutdowns that we then explore based on a systematic qualitative comparative analysis of all elections in SSA countries in 2014, 2015, and 2016. Our findings suggest that ISP ownership structure varies both within and across countries, and that such patterns of variation can indeed explain the (non-)occurrence of shutdowns. Finally, we discuss the role of ownership of Internet infrastructure more broadly and appeal for a shift in the unit of analysis when doing research on Internet control.

Internet Shutdowns in Election Times

Elections are generally regarded as procedural instrument by which political authority and legitimation is periodically and formally granted to elected representative(s). Yet holding elections does not mean that a country is democratic. In liberal democracies, elections serve as viable means of ensuring the orderly process of alternation in power; in authoritarian regimes, however, they are commonly established as a means by which the incumbent rulers hold onto power. Here, "elections are generally about access to state resources, rather than a competition over the rules of the game" (Gandhi & Lust-Okar, 2009, p. 412). In any case, calling elections is risky, given the uncertainty regarding their outcome; "the succession moment is normally the most dangerous recurring one in all political systems" (Rapoport & Weinberg, 2007, p. 15; cf. Hafner-Burton, Hyde, & Jablonski, 2014, p. 155). It requires that an incumbent accepts electoral defeat and actually steps down from power—a behavior, that is not a given in nondemocratic or democratizing contexts.

In consequence, authoritarian rulers often, but not always, manipulate elections to ensure their prolonged rule. They seek to incarcerate key opposition leaders and their supporters, ban their parties, and repress the media, among others (Gandhi & Lust-Okar, 2009). In their fear of losing power as the result of an election, they willingly risk the outbreak of conflict, if not violence. On the one hand, authoritarian incumbent leaders and ruling party agents often employ or threaten violence against opposition parties and their supporters, before or after elections. On the other hand, electoral malpractice—including voter intimidation, vote buying, and ballot fraud—is known to undermine public confidence in the credibility of elections; hence, opponents may be motivated to resort to conflict, violence, and threat as a means to determine, delay, or otherwise influence the results of the elections (Hafner-Burton et al., 2014, p. 154). In short, election violence and fraud often trigger protest against the handling or outcome of the election by opposition forces; such protests can, in turn, provoke the use of more state violence in an effort to dissolve public dissent and stay in power (Tucker, 2007).

Yet opposition forces face a typical collective action problem in authoritarian contexts. Mass protests are often prevented by the inability of opponents to effectively organize and communicate, that is, to locate and contact appropriate participants, to motivate them to make private resources publicly available, to persuade them to remain involved despite short-term setbacks and long-term risks, and to coordinate their efforts productively. Still, it is not simply the likely punishment for dissent given the degree of control and repression that prevents individuals from taking to the streets and challenging the political authority and legitimation of the incumbent ruler. Authoritarian regimes typically restrict traditional broadcast and print media in ways that make it difficult for citizens to coordinate effective collective opposition or to express their dissent in the public sphere (Gandhi & Lust-Okar, 2009; Tucker, 2007).

In the digital age, information and communication technologies (ICT), in particular the Internet, are said to help to overcome the coordination problem in at least two ways (Rød & Weidmann, 2015). First, the Internet provides opportunities to expose human rights violations and political misbehavior, such as electoral misconduct, and inform both internal and domestic audiences about what is happening. At the same time, it lowers the costs of acquiring independent information, including about a regime's stability and repressive capacities, the success of protests against related grievances, and how things ought to be done, such as the orderly conduct of elections elsewhere. Second, the Internet can facilitate the mobilization for and organization of protests under authoritarian rule in that it allows the transmission of information directly to like-minded citizens. It can hence be a powerful tool for opposition elites seeking to spread their political agenda and/or organize antiregime demonstrations. In short, according to these observers, the Internet can undermine authoritarianism by offering new communication channels that are "fundamentally resistant to state regulation, reducing a state's capacity for repression by hindering its ability to control the flow of information and political communication" (Garrett, 2006, p. 220).

At the same time, scholars recognize the incumbents' attempts to combat protests using ICT, or enabling its use by protesters (Deibert, Palfrey, Zohozinski, & Zittrain, 2008; Eyck, 2001; Weber, 2011). One of the most extreme forms of rendering control over digital information and communication are Internet shutdowns (Howard, Agarwal, & Hussain, 2011), that is, the "intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location" (Access Now, 2016, para. 1). These temporary blackouts have severe consequences for opposition groups' capabilities to effectively use digital communication and information channels. For instance, they prevent ordinary Internet users from accessing any websites, including online news portals or social media platforms; protesters can also no longer use coordination tools, such as online mapping services, like Google Earth and Google Maps, which are handy to effectively navigate through militarily occupied zones. They also cripple The Onion Router, known as TOR, an anticensorship tool that technical experts and activists often use to circumvent social media blocks.

How can a state go about shutting down the Internet? Despite its decentralization, the Internet relies on some fairly significant hierarchical structures, mostly for the sake of efficiency. It is specifically the physical infrastructure that, connecting the individual customer to the Internet, is key to controlling the flow of digital information and communication. Service providers with control over the physical infrastructure can extend that control into applications and content. Eventually, a digital video can only be posted to a website in cyberspace, such as a social media platform like Facebook, as long as the computers remain connected to the Internet. Hence, a government's ability to control the Internet primarily depends on its control of the ISP that grants Internet access to customers on its territory. There are different technical ways that ISPs can comply with a government request to disrupt the Internet. For instance, the ISP can simply power down devices, change the routing tables in such a way that packages of data cannot reach their goal, or stop resolving addresses that belong to a certain domain name system, such as that of the concerned country (e.g., .ug for Uganda). In short, while access to the Internet and its use depend critically on the permission and support of the domestic government (Milner, 2006), governments cannot directly restrict Internet access, but rely on the compliance of ISPs to halt their services.

State Control and Ownership of the Internet's Physical Infrastructure

Scholarship on the relationship between technologies, governments, and other political actors that attempt to influence technology adoption established the argument that technology has politics.

Challenging the supposed neutrality of technical artifacts, such as the provision of the Internet, the concept has been used to "refer to the strategic practice of designing or using technology to constitute, embody, or enact political goals" (Hecht, 2001, p. 256). Eventually, "arrangements of technical architecture are inherently arrangements of power" (DeNardis, 2012, p. 721). Our research borrows from this strand of literature by taking into consideration how technology can become an instrument of politics and how technological opportunities can shape political ambitions and actions (Gagliardone, 2016). From this perspective, technical artifacts such as the provision of Internet services—or its interruption—can be seen as vehicles for exercising power.

Indeed, the connection of an ISP to the rest of the network presents a bottleneck that is relatively easy to cut off or seize control over. The Internet connects thousands of ASs that are tasked with routing; that is, ASs manage unique sets of customers' Internet protocol (IP) addresses to and from which they carry traffic. We focus on ASs that are administered by commercial ISPs that operate on the given state territory and provide Internet connectivity to the larger population. They can be seen as centralized points of control or "gatekeepers" of the Internet as they control the gateway through which data flow in and out (DeNardis, 2014, p. 11).

Although we acknowledge that privately owned ISPs may vary in their willingness to follow government orders to shut down the Internet, in this article, we focus on the role of state majority ownership as the most immediate, physical form of state control. Eventually, both legal or regulatory control through the threat of revoking the license to operate as well as technical control over the traffic transiting the physical lines become obsolete if (at least considerable parts of) the physical infrastructure is in the hands of the state. We expect a company's commitment to comply with a government's request to shut down its services to be decisively determined by its ownership, notably, facilitated by state majority ownership and hindered otherwise.

Note that the ownership of a company (i.e., shareholders) is different from the management of the company (i.e., the CEO).[2] Some scholars see a company principally as a machine for making profits, where owners have no incentive to get involved in the management because of the uncertainty of benefits from doing so (Berle & Means, 1967). This strand of literature tends to disregard the role of ownership in management. Others find that control is well exerted by the owners, in particular through their voting rights but also through informal influence, such as during general assemblies or informal meetings with the management teams. According to this position,

> The role of shareholders is to determine all questions that are not routine, that cannot be decided by management because they are relevant to the relationship between the company and the capital market, and these include all fundamental matters affecting it. (Leech, 2002, p. 2)

[2] The border between ownership and management of a company can be blurred, such as in the case of family enterprises (Lemos & Scur, 2018).

We follow the second line of understanding and acknowledge that a company's owner can have substantial influence on its policies by actively engaging with management and voting their shares. We expect ISP majority ownership to be associated with the temporary interruption of access to the Internet in autocracies (in contrast to democracies), in particular if election periods are marked by violence.

Research Design and Operationalization of Variables

Focusing on SSA, we selected all countries[3] with presidential or parliamentary elections in 2014, 2015, or 2016, according to data provided by the Varieties of Democracy project (V-Dem; Coppedge et al., 2017). We limit our sample to countries during electoral periods, to hold the chances for mobilization (and hence shutdowns) constant. Our analysis covers the entire population, that is, all SSA countries where national elections took place (*N* = 33); any potential bias in case selection is thereby minimized. As Table 1 demonstrates, the occurrence of Internet shutdowns at election times varies, with elections being accompanied by shutdowns in 10 of these 33 cases, as does the presence of ISP state majority ownership, the occurrence of electoral violence, and the regime type.

Table 1. Calibrated Data.

Case (Country–Election Year)	ISP State Ownership	Autocracy	Electoral Violence	Internet Shutdown
Benin 2015	1	0	0	0
Benin 2016	1	0	0	0
Botswana 2014	1	0	0	0
Burkina Faso 2015	0	0	0	0
Burundi 2015	1	1	1	1
CAR 2015	0	1	0	0
CAR 2016	0	0	0	0
Chad 2016	1	1	1	1
Djibouti 2016	0	1	1	1
Equatorial Guinea 2016	1	0	0	0
Ethiopia 2015	1	1	0	1
Gabon 2016	1	1	0	1
Gambia 2016	0	0	1	1
Ghana 2016	1	1	0	1
Guinea 2015	0	0	0	0
Guinea-Bissau 2014	1	0	0	0
Ivory Coast 2015	0	0	0	0

[3] Except for São Tomé and Mauritius, because no data on ISP ownership are available for the African islands, but Madagascar.

Case (Country–Election Year)	ISP State Ownership	Autocracy	Electoral Violence	Internet Shutdown
Ivory Coast 2016	0	0	0	0
Lesotho 2015	1	0	0	0
Malawi 2014	0	0	0	0
Mauritania 2014	0	0	0	0
Mozambique 2014	0	1	0	0
Namibia 2014	1	0	1	0
Niger 2016	1	0	0	0
Nigeria 2015	1	0	0	0
Republic of Congo 2016	1	0	0	0
South Africa	1	0	0	0
Sudan, North 2015	0	1	1	1
Tanzania 2015	1	0	1	0
Togo 2015	1	1	0	1
Uganda 2016	0	1	1	1
Zambia 2015	1	0	0	0
Zambia 2016	1	0	1	0

Note. Raw data are provided in Online Appendix 1, which can be downloaded from the author's website (http://www.tina-freyburg.eu/1/135/resources/publication_2903_1.pdf).

To probe the plausibility of our argument, we use crisp-set qualitative comparative analysis (csQCA), which is an analytical technique to uncover empirical patterns in data by examining set-theoretic relationships between causally relevant conditions following a deterministic logic of causation (Schneider & Wagemann, 2010). This research method is adequate because we are interested in the effect of a dichotomous condition (state majority ownership vs. no state majority ownership) on a dichotomous outcome (occurrence vs. nonoccurrence of an Internet shutdown). CsQCA links binary-coded conditions and outcomes through set-theoretical relations by classifying their presence (= 1) and absence (= 0) for each case. Based on Boolean methods of logical comparison (i.e., the algebra of logic and set-theoretical relationships), csQCA is therefore appropriate not only to check the necessity and sufficiency of conditions but also to identify more than one path leading to the same outcome.

Our outcome is the occurrence or nonoccurrence of an Internet shutdown during election periods (i.e., shortly before, during, or shortly after polling day). Defined as "intentional disconnections of digital communications by government authorities" (Wagner [2018], this Special Section; cf. Access Now, 2016), shutdowns can be considered as an extreme form of censorship. Looking specifically at politically motivated Internet shutdowns during election times enables us to differentiate simple technical failures from "the intent of a governmental actor to disconnect networks" (Wagner [2018], this Special Section). Because governments now have the ability to apply shutdowns and other restrictions in a more targeted manner, and authorities commonly cut off specific regions in response to local instability, dissent, or insecurity, we apply a more comprehensive understanding of Internet shutdowns than Ben Wagner's. Specifically, we count as a shutdown any considerably disrupted access to the Internet in a country, including the targeted blocking of particularly prominent global platforms commonly used for mobilization and campaigning purposes (e.g., WhatsApp, YouTube, Facebook, Twitter), and the intentional slowing down of connections or of a specific protocol or resource (i.e., "throttling"; Aceto & Pescape, 2015). Note that full Internet shutdowns are often employed at a subcountry level (e.g., state, city, province, neighborhood) and may not involve all ISPs providing Internet services within a state's territory. Data come predominantly from the Access Now platform in the context of its #KeepItOn initiative and is complemented with information from the global news database Factiva. Restricting the time period of interest to the year of the election, we used the following search strings for each country: *country AND elections AND [Internet OR access] AND [shutdown OR blocked]*.

In two of the cases, 2015 Ethiopia and 2016 Equatorial Guinea, the occurrence of an Internet shutdown was not as clear as in the rest. Both countries feature in several lists as among the most censored countries in the world; Internet and mobile phone networks are repeatedly disrupted, and social media, circumvention tool websites, and communications platforms are temporarily blocked time and again (e.g., Freedom House, 2015; U.S. Department of State, 2017a, 2017b). Because both countries constantly face a high level of Internet filtering and manipulation, it is difficult to assess whether the blocking of access to the Internet in the run-up to the general elections is directly linked to the elections. As the given sources support a temporary halt of services, we code an Internet shutdown as present for both.

Our main condition of interest is state control of ISPs by means of majority ownership. We draw on the definition of owners as pivotal actors based on the size of owned shares (Leech, 2002). By virtue of controlling more than half of the voting interests in the company, the majority shareholder has decisive influence in the business operations and strategic direction of the company. Setting the full control threshold conservatively, we avoid any potential inconsistencies emerging from the competition for control. We distinguish between ISPs for which the state holds the majority of outstanding shares (i.e., 51% or more), and those for which it holds fewer or no shares. States tend to be the majority shareholder of those ISPs that provide the national Internet backbone and may operate key infrastructure within a country that is used by other ISPs as well (Warf, 2011). In Cameroon, for instance, the state-owned ISP CamTel runs crucial parts of the national fiber backbone on which other providers rely to service their subscribers. Even if the state is the majority shareholder of only one small ISP out of many operating on its territory, then by having direct access to key parts of the Internet infrastructure, it can paralyze the provision of Internet access in a country. Against this, we code this condition with 1 if there is at least one ISP of which the state is the majority shareholder, and with 0 otherwise.

We draw on an original data set covering all telecommunications companies that hold official state licenses to operate cables and provide Internet services (Freyburg et al., 2018). Data come from financial-analysis tools (e.g., Eikon [http://eikon.thomsonreuters.com] and Orbis [https://orbis.bvdinfo.com]), specialized blogs (e.g., Research ICT Africa [https://www.researchictafrica.net]), news websites such as All Africa (http://allafrica.com) and Quartz Africa (https://qz.com/Africa), and Bloomberg Snapshot repositories (https://www.bloomberg.com). This information is triangulated with the annual reports provided by the telecommunications companies and data from market research and analysis companies, in particular, African Telecommunications News (AMETW; https://www.africantelecomsnews.com) and TeleGeography (https://www.telegeography.com).

We further include a country's regime type. Existing studies claim the manipulation of Internet access to be more prevailing in autocracies (Deibert et al., 2008; Howard et al., 2011). To determine categorically whether a regime is an autocracy or a democracy, we use Ulfelder's (2007) two-component measure that corresponds to common understanding of an electoral democracy. It has not only been shown to be particularly useful for Africa (Bogaards, 2012) but also avoids conceptual overlaps with our third condition, election violence. The selected Polity IV component variables are executive recruitment (EXREC) and the competitiveness of political participation (PARCOMP; Marshall et al., 2017). In line with Ulfelder (2007), we identify a regime as democracy (= 0) if it provides "some contestation in the selection of the chief executive (EXREC > 5) and do[es] not substantially restrict political participation (PARCOMP >2 or = 0)" (p. 1001); when a regime falls short on one or both dimensions, we categorize it as autocracy instead (= 1). By determining the democratic minimum for each of the Polity component variables, we avoid not only the problem of concept-measure inconsistency but the logic behind the minimum as aggregation rule also matches the general configurational nature of our study.[4]

Our third and last condition is election violence. Elections in SSA are particularly delicate, with many countries still in a difficult process of transition where elements of democratic participation are intertwined with authoritarian rule and political repression. According to Lindberg (2004), 80% of African elections were accompanied by some kind of election-related violence in the late 1990s and early 2000s. To account for the role of violent protest, we use the V-Dem (v2elpeace) variable that captures whether "the campaign period, election day, and postelection process [were] free from . . .violence related to the conduct of the election and the campaigns (but not conducted by the government and its agents)" (Coppedge et al., 2017, p. 97). We use the ordinal variable variant and code "widespread violence," "significant levels of violence," as well as "some outbursts of limited violence" with 1, and the remaining two categories ("only a few instances of isolated violent acts," "no election-related violence") with 0.

ISP State Ownership and Internet Shutdowns in Africa

We use crisp-set QCA to establish whether particular configurations of conditions, namely national similarities and differences in Internet ownership structure, election violence, and regime type, can be linked to the (non-)occurrence of Internet shutdowns. Table 2 and Table 3 show the parsimonious solution based on our dichotomized data. All the conditions in the parsimonious solution generally show the expected direction. For each outcome, the occurrence (= positive) and the nonoccurrence (= negative) of an Internet shutdown, there are two sufficient conjunctions, each covering part of the empirically observed configurations. They are displayed with a logical OR relation, either one being sufficient for some of the configurations, but both are necessary to cover all of them.

[4] ISPs are not more likely to be majority owned by the state if the country is ruled autocratically, $r(31) = -.24$, $p = .81$.

The results of the csQCA support our general expectations. As to the negative outcome (*N* = 23), if the state holds no majority of shares from at least one ISP, then we also observe no Internet shutdown in the absence of election violence. That is, the absence of election violence and the absence of ISP state majority ownership are together sufficient for the absence of Internet shutdowns, independent of the regime type (39%). Plus, if the state is majority owner but democratically constituted, then we also observe no Internet shutdowns during election times, regardless of how violent they are. We therefore observe several democracies, 14 to be exact (61%), in which ISPs are majority owned by the state but no Internet shutdowns occurred during election times (see Online Appendix 2; http://www.tina-freyburg.eu/).

Table 2. csQCA Output—Parsimonious Solution for Internet Shutdowns (Negative Outcome).

Cases	**Conditions**			**Coverage**	**Consistency**
	ISP State Ownership	*Autocracy*	*Electoral Violence*	*Raw/Unique*	
Burkina Faso_2015, CAR_2016, Ghana_2016, Guinea_2015, Ivory Coast_2015, Lesotho_2015, Malawi_2014; CAR_2015, Mauritania_2014	○		○	.39	1.0
Benin_2015, Benin_2016, Botswana_2014, Djibouti_2016, Guinea-Bissau_2014, Ivory Coast_2016, Namibia_2014, Niger_2016, Nigeria_2015, Zambia_2015; Mozambique_2014, South Africa 2014, Tanzania_2015, Zambia_2016	●	○		.61	1.0
Solution	isp * violence + ISP * autocracy <=> shutdown			1.0	1.0

Note. Empty circles depict the absence of the condition, shaded circles its presence. In line with Boolean operators, uppercase letters indicate the presence of an outcome or a condition, and lowercase letters indicate their absence; * designates logical AND, while + designates logical OR, and the logical (set-theoretical) relation <=> signals both necessity and sufficiency; solution coverage and consistency (inclusion) for both paths is 1.000; all cases are uniquely covered.

If we turn to the positive outcome (*N* = 10), again, one solution with two conjunctions is suggested. If the state is the majority owner of at least one ISP and an autocracy, then we observe an Internet shutdown, regardless of election-related violence (60%). However, if the state is no majority shareholder but elections are marked by violence, then we can observe shutdowns, too. The latter conjunction refers to four cases, namely Gabon in 2016, the Republic of Congo in 2016, North Sudan in 2015, and Uganda in 2016—that is, three autocracies but one democracy: Gabon. In other words, and unexpectedly, a democracy in which the state is no majority shareholder of any ISP company shows a positive outcome. Global democracy measures, notably Freedom House's Freedom in the World and Polity's Institutionalized Autocracy, rate 2016 Gabon as autocracy (i.e., with "not free" and at −0.5, respectively), however. We therefore re-run our analysis with Gabon recoded as autocracy; the dominant tendency remains unchanged (Online Appendix 3; http://www.tina-freyburg.eu/1/135/resources/publication_2903_1.pdf).

Table 3. csQCA Output—Parsimonious Solution for Internet Shutdowns (Positive Outcome) .

Cases	**Conditions**			**Coverage**	**Consistency**
	ISP State Ownership	*Autocracy*	*Electoral Violence*	*Raw/Unique*	
Equatorial Guinea_2016, Ethiopia_2015, Gambia_2016, Togo_2015; Burundi_2015, Chad_2016	●	●		.60	1.0
Gabon_2016; Republic of Congo_2016, Sudan-North_2015, Uganda_2016	○		●	.40	1.0
Solution	ISP * AUTOCRACY + isp * VIOLENCE <=> SHUTDOWN			1.0	1.0

Note. Empty circles depict the absence of the condition, shaded circles its presence. In line with Boolean operators, uppercase letters indicate the presence of an outcome or a condition, and lowercase letters indicate their absence; * designates logical AND, while + designates logical OR, and the logical (set-theoretical) relation <=> signals both necessity and sufficiency; solution coverage and consistency (inclusion) for both paths is 1.000; all cases are uniquely covered.

Still, the remaining cases—Sudan (North) 2015, the Republic of Congo 2016, and Uganda 2016—work against our expectation that state majority ownership of at least one ISP is necessary to explain the occurrence of Internet shutdowns. We therefore zoom in to the ISP ownership structure of two of these cases, Uganda and the Republic of Congo, to better understand the relationship between the state and the ISP on its territory.[5] What features might have facilitated ISP compliance with the government's request to interrupt the provision of Internet services?

The Republic of Congo and Uganda: The Role of Private Ownership

Both the Republic of Congo's 2016 presidential election and Uganda's 2016 general elections were marked by Internet shutdowns in the context of election violence, but no major state involvement in ISP. According to the French news agency Agence France-Presse, Congo's interior minister Raymond Mboulou urged the ISP on the country's territory to shut down their services for "reasons of security and national safety" ("Congo Holds Elections," 2016). The country experienced an outbreak of election violence after president Denis Sassou-Nguesso secured a third term in the presidential elections, thereby extending his 32-year rule "over the oil-rich, but poor nation" ("Congo in Media Blackout," 2016). Likewise, in February 2016, the Ugandan government ordered a shutdown of major social media platforms like Facebook, Twitter, and WhatsApp on polling day, officially pronounced as a "security measure to avert lies" (Duggan, 2016, para. 4). The electoral period had been tense, with rampant voter intimidation and harassment, and protesters and opposition supporters having frequently been met with armed security forces.

In the Republic of Congo (Brazzaville), only three licensed ISPs operate on Congolese territory, namely Airtel Congo, Equateur Telecom Congo (formerly Azur Congo), and MTN Congo. This clearly highlights the lack of diversity in the Congolese ISP landscape, making it more susceptible to government manipulation. Moreover, all of the ISPs are in the hands of private investors from emerging economies. Airtel Congo and MTN Congo belong to the major multinational corporations and leading emerging market telecom operators Bharti Airtel in India and MTN in South Africa, respectively. Both internationally operating companies have chosen to invest in emerging economies on the African continent with its billion-plus population, attracted by the growth of the sector (Schoentgen & Gille, 2017). The third ISP—Equateur Telecom Congo—is owned by Congolese private investor Jean Bruno Obambi. Even though little is known about Obambi, he belongs to a family of businessmen that is said to have close ties to the ruling elite of Sassou-Nguesso (Africa Intelligence, 2016).

In Uganda, in turn, the ISP landscape is more diverse, with no less than eight different licensed ISPs. Seven of them belong to non-Western shareholders, whereas the eighth ISP—Vodafone Uganda—primarily belongs to companies based in the United Kingdom and the Netherlands. While all major ISPs, including MTN, Airtel, Smile, and UTL shut down their services, it was precisely Vodafone Uganda whose connectivity remained functional ("Govt Blocks Facebook, Twitter," 2016). This suggests that the cooperation of ISPs to shut down their services on request may depend on company-specific characteristics, such as their ownership. While similarly to Congo Brazzaville, Bharti Airtel and MTN have

[5] The ownership structure in North Sudan resembles the Congolese one, with four licensed ISPs owned by private investors from emerging or oil-rich Middle East economies, namely Canartel, MTN Sudan, Sudatel, and Zain Sudan.

major shares in two of the ISPs (Africell and MTN Uganda, respectively), the other affected ISPs belong to different private and nonprivate shareholders. Smile, an ISP mainly servicing bigger urban regions in Uganda, is owned by a shareholder based in Mauritius, with several traces going back to investors in Saudi Arabia, Nigeria, and South Africa. The main share (69%) of UTL, on the other hand, belongs to the Libyan company LAP Green that is run by the Libyan government, whereas the minor share (31%) belongs to the Ugandan government. UTL is one of the biggest ISPs servicing large parts of the Ugandan population. This suggests that UTL alone has already a major impact in terms of providing and hence cutting access to the Internet. This finding is strengthened by recent developments taking place in Uganda. After the Libyan shareholder faced major difficulties in injecting capital in the ailing company, the Ugandan state has announced to take over UTL ("Uganda Government." 2017). This may suggest that the Ugandan government tries to regain control over the telecommunications infrastructure as UTL operates important parts of the national communication backbone. Even though the state government holds no majority of shares in any of the ISPs involved in the Internet shutdowns, the ownership patterns in the Republic of Congo and Uganda seem to have facilitated their occurrence.

A closer look at the ownership patterns in 2016 Congo (Brazzaville) and in 2016 Uganda hence reveals that private ISPs may have varying motivations for cooperating with the government, and that some ISPs face higher stakes for participating in a shutdown than do others. Eventually, private ISPs can be domestic or foreign, and the latter can be dominated by investors with headquarters in countries that vary in terms of their level of democraticness or the expansion strategies of their economies, among others. The two case studies further suggest that there is no need for direct state control through majority ownership if the majority of ISPs operating on state territory are owned by foreign companies from fast-growing developing countries with ambitious expansion strategies, such as India or South Africa; by private companies with investors from authoritarian regimes, like Saudi-Arabia and Libya; or by private domestic companies with close ties to the ruling elite. Overall, it appears worth exploring further the different types of private ownership and their effects on a state's capacity to use ICT for repressive purposes.

Discussion and Outlook

Although state involvement in ISPs can be used straightforwardly by governments to render control over Internet access, the situation becomes multidimensional once private ISPs are involved. Setting up telecom infrastructure is costly (Andoh-Baidoo, Osatuyi, & Kunenen, 2014); states often need to rely on foreign investment to foster Internet-based economic growth. If a digitally repressive state decides to not only keep the communication borders open but also accept foreign investment, the most direct way of controlling the Internet infrastructure through state ownership is no longer available. Rather, the incumbent government depends on (foreign) private telecom companies in its efforts to control Internet-based information and communication. In an attempt to solve the alleged "dictator's dilemma," state governments often require—by law or voluntary agreement—that ISPs assist upon request in interrupting Internet services, restricting specific Internet content, and providing user-identifying information, among others. As part of their license agreement, ISPs hence often agree on potentially being willing to temporarily shut down their services on government request.

In consequence, a company can become subject to two potentially conflicting laws: the local law requiring compliance with government requests, and a national law. Compliance with a government request to interrupt services should depend on where a company's shareholders are mainly based. If the majority shareholders have headquarters in established democracies, national laws may comprise (international) human rights standards. In May 2015, United Nations (UN) Special Rapporteur on Freedom of Opinion and Expression, together with experts from relevant other organizations, issued a declaration that Internet kill switches are impermissible under international human rights law, even in times of conflict (Article 19, 2015). According to this declaration, governments can no longer justify ordering telecommunications companies to shut off Internet services in the face of social unrest or protest. Telecom companies hence face a choice between strained ties with the host government or public condemnation, if not persecution at home (Lecraw, 1984, p. 27). We would hence expect companies with roots in established democracies to be less willing to comply with an authoritarian state's order to interrupt or manipulate their services to repress political opposition or prevent protests.

Recent events support this expectation. The Telecommunications Industry Dialog, for instance, is a group of eight multinational companies with headquarters in European democracies and the United States who jointly address freedom of expression and privacy in the sector.[6] All European dialogue members also joined the expanded Global Network Initiative (GNI) in 2017. These companies have committed to the GNI Principles on freedom of expression and privacy and agreed to collaborate with academics, civil society organizations, and investors to further their efforts to advance privacy and freedom of expression in the ICT sector. Prominent examples of such efforts to minimize complicity in government censorship and other abuses include Vodafone's (2014) transparency reports detailing the type and number of requests it receives from government bodies. These company reports are meant to not only compensate for gaps in the national governance of governmental surveillance activities but also to regain trust from customers.

Results from Ranking Digital Rights (2017) support that ISPs from emerging markets are less sensitive when it comes to public commitments and disclosed policies protecting users' freedom of expression and privacy. While the big Western multinationals (AT&T, Vodafone, Orange and Telefonica) place first, ISPs from emerging markets, notably the Indian Bharti Airtel or South Africa-based MTN perform hardly any better than Malaysian Axiata and only slightly better than Etisalat from the United Arab Emirates. The Indian and South African governments also joined the group of countries, including Russia, China, and Saudi Arabia, that opposed the 2016 resolution of the United Nations Human Rights Council condemning "unequivocally measures to intentionally prevent or disrupt access to or dissemination of information online" (2016). The point of contention for these countries was the line condemning any intentional disruption to Internet access or infringement on the ability to share information online, which they asked to be deleted. Eventually, the UN resolution, though nonbinding, stands in direct opposition to recent government actions to intentionally prevent access to the Internet. Overall, it appears that foreign companies from emerging markets are willing to accept restrictions on their service provisions because of

[6] These companies are AT&T (United States); Millicom, Nokia, Telia, and Telenor Group (all Scandinavia); Telefonica (Spain); Orange (France); and Vodafone (UK).

competitive necessity, in particular if the new market abroad is crucial in terms of size and geographical location.

As this discussion demonstrates, instances of Internet shutdowns raise concerns about various values, including freedom of expression, commerce, public safety, and law enforcement. They raise questions about the conditions under which government-requested interruption of Internet services is (perceived as) legitimate. Universal Internet outages in a country such as Egypt might be rejected as technological repression violating basic human rights by the same citizen who accepts it in other circumstances, despite the collateral damage to free expression, commerce and possibly public safety. An example for a scenario potentially perceived as appropriate would be government authorities in a country such as the United Kingdom cutting off Internet services in a location allegedly targeted by a planned terrorist attack that is said to be coordinated by social media. "More than anything, these instances are a reminder that infrastructure is not a given and can be severed by governmental action" (DeNardis, 2012, p. 731).

Conclusion

Despite its allegedly decentralized nature, the Internet relies on a hierarchical physical infrastructure that provides for opportunities to control and manipulate the flow of digital information and communication. The arguably most brute force method of Internet control is a temporary shutdown. Between 2014 and 2016, access to the Internet was restricted during about one third of the elections in SSA countries. Typically, these intentional disruptions were ordered by the incumbent rulers to prevent opponents from organizing protests or reporting election malfeasance. Yet the government usually cannot directly interrupt Internet access but relies on the willingness of ASs, in particular ISPs, to halt their services. ASs can be seen as bottlenecks of the Internet, as they form central points through which data flow in and out for a larger population. Especially in Africa, cutting last-mile access can be efficient as there are only few ASs that control all IP addresses within a country. Most ASs belong to ISPs owned by the state and/or private investors. In this article, we argued that ISP ownership is critical to understanding authoritarian practices violating citizens' freedom of expression in the digital sphere.

Specifically, we studied the link between Internet shutdowns and state majority ownership of ISPs at the time of general elections in any SSA country between 2014 and 2016. Our csQCA of original data on ISP ownership structures and documented Internet shutdowns revealed a positive relationship between companies majority owned by an authoritarian state and a temporary halt of Internet provision during electoral periods. On the one hand, our findings demonstrate that election violence alone is insufficient to explain Internet shutdowns ordered by the government. On the other hand, it turns out that neither is state majority ownership of ISPs sufficient to explain why some autocracies interrupt access to the Internet and others did not. Case studies of Uganda and the Republic of Congo's 2016 elections highlighted that shutdowns can also occur in the absence of state majority ownership when private ISPs are willing to comply with a government request to halt their services. In particular, our analysis suggests that Internet shutdowns may be facilitated if ISPs are owned by private companies with investors from authoritarian regimes like Saudi Arabia and Libya, with their headquarters in fast-growing developing countries, such as India or South Africa, or private companies whose owners are close to the ruling elite.

While the mechanism of state-owned ISPs and Internet disruptions appears to be straightforward, further research needs to determine the circumstances under which ISPs owned by private investors comply with government requests to restrict their services.

The structure of private ownership is arguably complex and may serve various goals, including optimizing taxation or "blurring" accountability. Although the configurational analysis is useful to get a better understanding of the relevance of the ownership variable, it does not allow capturing the multidimensionality of the real-world situation. That is, by aggregating our company-level data at the macro level of countries, we lose much information about the ownership structure of different companies within the same country, including whether the mother shareholder of a foreign company is based in a democratically constituted country, or not. To adequately account for the effects of different ownership structures on the likelihood of ICT use for repressive purposes, however, it appears to matter whether a mother company (e.g., Vodafone with its headquarter in the United Kingdom) can be held accountable for the action of those companies in which it holds shares. Also, the size of the market, in which a shareholder invests, and potential future profits seem to play a role when it comes to a company's willingness to cooperate with governments. In addition, upcoming large-*N* studies should also systematically account for temporally and spatially varying levels of Internet penetration, in terms of political relevance for protest mobilization, but also economic damage in consequence of a shutdown. Overall, the structure of shareholders is more complex than the presented analysis at the country level suggests; longitudinal comparative studies at the level of companies are needed. These considerations call for further research on the role of private ownership of ISPs in authoritarian contexts.

References

Access Now. (2016). *#KeepItOn. Fighting Internet shutdowns.* Retrieved from https://www.accessnow.org/keepiton/

Aceto, G., & Pescapé, A. (2015). Internet censorship detection: A survey. *Computer Networks*, *83*, 381–421.

Africa Intelligence. (2016). *Paul Obambi, the man at the top of Congo-B's private sector tree.* Retrieved from https://www.africaintelligence.com/aia/insiders/congo-b/2016/01/19/paul-obambi-the-man-at-the-top-of-congo-b-s-private-sector-tree/108125864-be1

Albiman, M., & Sulong, Z. (2016). The role of ICT use to the economic growth in sub-Saharan African region. *Journal of Science and Technology Policy Management*, *7*(3), 306–329.

Andoh-Baidoo, F., Osatuyi, B., & Kunenen, K. (2014). ICT capacity as the investment and use of ICT: Exploring its antecedents in Africa. *Information Technology for Development*, *20*(1), 44–59.

Article 19. (2015). *Joint declaration on freedom of expression and responses to conflict situations.* Retrieved from https://www.article19.org/resources/joint-declaration-freedom-expression-responses-conflict-situation/

Berle, A., & Means, G. (1967). *The modern corporation and private property*. New York, NY: Transaction Publishers.

Bogaards, M. (2012). Where to draw the line? From degree to dichotomy in measures of democracy. *Democratization*, *19*(4), 690–712.

Central African Republic candidates call for halt to "tainted" election. (2016, January 4). *The Guardian.* Retrieved from https://www.theguardian.com/world/2016/jan/04/central-african-republic-candidates-call-for-halt-to-tainted-election

Congo holds elections under telecom blackout. (2016). *France 24*. Retrieved from http://www.france24.com/en/20160320-congo-brazzaville-holds-elections-under-telecom-blackout-nguesso

Congo in media blackout for presidential elections. (2016b, March 20). *Al Jazeera.* Retrieved from http://www.aljazeera.com/news/2016/03/congo-media-blackout-presidential-elections-160320044041238.html

Coppedge, M., Gerring, J., Lindberg, S., Skaaning, S.-E., Teorell, J., Altman, D., . . . Staton, J. (2017). *V-Dem codebook v7.1 Varieties of Democracy (V-Dem) Project* [Data set and code book]. Retrieved from https://www.v-dem.net/en/data/data-version-7-1/

Corrales, J., & Westhoff, F. (2006). Information technology adoption and political regimes. *International Studies Quarterly*, *50*(4), 911–933.

Dasgupta, S., Lall, S., & Wheeler, D. (2005). Policy reform, economic growth and the digital divide. *Oxford Development Studies*, *33*(2), 229–243.

Deibert, R., Palfrey, J., Zohozinski, R., & Zittrain, J. (2008). *Access denied: The practice and policy of global Internet filtering.* Cambridge, MA: MIT Press.

DeNardis, L. (2012). Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society*, *15*(5), 720–738.

DeNardis, L. (2014). *The global war for Internet governance*. New Haven, CT: Yale University Press.

Duggan, B. (2016, February 19). Uganda shuts down social media; candidates arrested on election day. *CNN*. Retrieved from http://edition.cnn.com/2016/02/18/world/uganda-election-social-media-shutdown/index.html

Eyck, T. (2001). Does information matter? A research note on information technologies and political protest. *The Social Science Journal*, *38*, 147–160.

Freedom House. (2015). Ethiopia. Freedom on the net. Retrieved from https://freedomhouse.org/sites/default/files/resources/FOTN%202015_Ethiopia.pdf

Freyburg, T., Garbe, L., & Wavre, V. (2018). *Who owns the Internet, and why does it matter? A new dataset on Internet infrastructure and ownership of Internet service providers in sub-Sahara and North Africa, 2000–2016.* Paper presented at the 2018 ISA (April 4–7, San Francisco) and MPSA (April 5–8, Chicago) conferences.

Gagliardone, I. (2016). *The politics of technology in Africa*. Cambridge, MA: Cambridge University Press.

Gandhi, J., & Lust-Okar, E. (2009). Elections under authoritarianism. *Annual Review of Political Science*, *12*, 403–422.

Garrett, K. (2006). Protest in an information society: A review of the literature on social movements and the new ICTs. *Information, Communication and Society*, *9*(2), 202–224.

Govt blocks Facebook, Twitter. (2016). *The Observer.* Retrieved from http://www.observer.ug/news-headlines/42668-govt-blocks-facebook-twitter-2

Hafner-Burton, E., Hyde, S., & Jablonski, R. (2014). When do governments resort to election violence? *British Journal of Political Science*, *44*(1), 149–179.

Hecht, G. (2001). Technology, politics, and national identity in France. In M. Allen & G. Hecht (Eds.), *Technologies of power* (pp. 253–294). Cambridge, MA: MIT Press.

Howard, P., Agarwal, S., & Hussain, M. (2011). When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review*, *14*(3), 216–232.

Hughes, T. (1983). *Networks of power: Electrification in Western society, 1880–1930*. Baltimore, MD: Johns Hopkins University Press.

Lecraw, D. (1984). Bargaining power, ownership, and profitability of transnational corporations in developing countries. *Journal of International Business Studies*, *15*(1), 27–43.

Leech, D. (2002). *Shareholder voting power and ownership control of companies* (Working Paper no. 564). Coventry, UK: University of Warwick.

Lemos, R., & Scur, D. (2018). *All in the family? CEO choice and firm organization* (Discussion Paper no 1528). London, UK: Centre for Economic Performance.

Levitsky, S., & Way, L. (2010). *Competitive authoritarianism: Hybrid regimes after the Cold War.* Cambridge, UK: Cambridge University Press.

Lindberg, S. (2004). The democratic qualities of competitive elections: Participation, competition and legitimacy in Africa. *Commonwealth & Comparative Politics*, *42*(1), 61–105.

Luong, P., & Weinthal, E. (2006). Rethinking the resource curse: Ownership structure, institutional capacity, and domestic constraints. *Annual Review of Political Science*, *9*, 241–263.

Marshall, M., Gurr, T., & Jaggers, K. (2017). *Political regime characteristics and transitions, 1800–2016* [Data set users' manual]. Vienna, VA: Center for Systemic Peace.

Milner, H. (2006). The digital divide: The role of political institutions in technology diffusion. *Comparative Political Studies*, *39*, 176–199

Odhiambo, S. (2017). Internet shutdowns during elections. *Africa Up Close.* Retrieved from https://africaupclose.wilsoncenter.org/internet-shutdowns-during-elections/

Olukotun, D. (2016). Victory! President of Ghana says no to Internet shutdowns during coming elections. *Access Now.* Retrieved from https://www.accessnow.org/president-ghana-says-no-internet-shutdown-elections-social-media/

Palinn, C. (2017). Internet control through ownership: The case of Russia. *Post-Soviet Affairs, 33*(1), 16–33.

Ranking Digital Rights. (2017). *The 2017 Ranking Digital Rights corporate accountability index.* Retrieved from https://rankingdigitalrights.org/index2017

Rapoport, D., & Weinberg, L. (2007). Elections and violence. *Terrorism and Political Violence*, *12*(3/4), 15–50.

Rød, E., & Weidmann, N. (2015). Empowering activists or autocrats? The Internet in authoritarian regimes. *Journal of Peace Research*, *52*(3), 338–351.

Schneider, C., & Wagemann, C. (2010). Standards of good practice in qualitative comparative analysis (QCA) and fuzzy-sets. *Comparative Sociology*, *9*(3), 397–418.

Schoentgen, A., & Gille, L. (2017). Valuation of telecom investments in sub-Saharan Africa. *Telecommunications Policy*, *41*(7/8), 537–554.

Stockmann, D. (2013). *Media commercialization and authoritarian rule in China*. Cambridge, UK: Cambridge University Press.

Tucker, J. (2007). Enough! Electoral fraud, collective action problems, and post-communist colored revolutions. *Perspectives on Politics*, *5*(3), 535–551.

Uganda government takes over troubled telecom. (2017). *The East African.* Retrieved from http://www.theeastafrican.co.ke/business/Uganda-government-takes-over-troubled-telecom/2560-3833146-8ojxtqz/index.html

Ulfelder, J. (2007). Natural-resource wealth and the survival of autocracy. *Comparative Political Studies*, *40*(8), 995–1018.

United Nations. (2016). *Oral revisions of 30 June.* Retrieved from https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

U.S. Department of State. (2017a). Country Reports on Human Rights Practices for 2017. Ethiopia. Retrieved from https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper

U.S. Department of State. (2017b). Country Reports on Human Rights Practices for 2017. Equatorial Guinea. Retrieved from https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper

Vodafone. (2014). *Country-by-country disclosure of law enforcement assistance demands*. Retrieved from http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

Wagner, B. (2018). Understanding Internet shutdowns: A case study from Pakistan. (This Special Section).

Warf, B. (2011). Geographies of global Internet censorship. *GeoJournal*, *76*, 1–23.

Weber, R. (2011). Politics through social networks and politics by government blocking: Do we need new rules? *International Journal of Communication*, *5*, 1186–1194.

Wegenast, T., & Schneider, G. (2017). Ownership matters: Natural resources property rights and social conflict in Sub-Saharan Africa. *Political Geography*, *61*, 110–122.

Weidmann, N. (2015). Communication networks and the transnational spread of ethnic conflict. *Journal of Peace Research*, *52*(3), 285–296.