

The Experience of Internet Freedom Among African Users

VALENTINA BAÚ¹

University of New South Wales, Australia

ENRICO CALANDRO

Research ICT Africa, South Africa

This article examines African Internet users' experience of online freedom to assess levels of trust and mistrust of the Internet in Africa. Internet users' perception of the protection or denial of their rights online—such as freedom of expression, privacy, and safety and security—in selected African countries is examined here as an outcome of constraining or enabling Internet policy and regulatory frameworks. Demand-side survey data collected via nationally representative ICT access and use surveys in 2017 is analyzed within the context of the Internet ecosystem as it plays out at the national level in three sub-Saharan African countries: Nigeria, Rwanda, and South Africa. Findings are contextualized within the framework of the Sustainable Development Goals, emphasizing the role that the Internet plays in contributing to the growth of a country when relevant policies are formulated in a way that addresses users' needs while safeguarding their rights.

Keywords: information and communication technologies, sub-Saharan Africa, Internet policy, Internet freedom, Sustainable Development Goals

From a rights and legal protection perspective, assumptions regarding international guidelines and good practice based on human rights, democratic principles, and the rule of law, which drive the development of specialized areas of cyberlaw, are not applicable in all African countries (Abdulrauf, 2018; Lumbu, 2018). Yet, there is very little evidence of research being conducted on Internet users' perception of freedom of expression in the African reality. Such research can not only facilitate the development of policies that improve Internet users' online experience, but also enhance its economic and social advantages.

Anecdotal evidence on Internet users' awareness of censorship (Bitso, 2014; Turianskyi, 2018) demonstrates the urgency for investigating this issue, not only through technical and legal instruments, but also through empirical policy analysis. To overcome these limitations in censorship studies, which typically

Valentina Baú: v.bau@unsw.edu.au

Enrico Calandro: ecalandro@researchictafrica.net

Date submitted: 2020–05–19

¹ The authors would like to acknowledge the International Development Research Centre (IDRC) for the funding received under the After Access research project to conduct the ICT Access and Use surveys.

Copyright © 2020 (Valentina Baú and Enrico Calandro). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at <http://ijoc.org>.

emphasize either technical censorship or legal restrictions to freedom of expression, an exploration of Internet users' perception of the fulfilment or denial of their rights online is needed.

The aim of this research report is to contribute to filling in this gap by examining African Internet users' experience of their freedom online, with the goal of providing evidence toward an assessment of levels of trust and mistrust of the Internet in Africa. The perception of Internet users regarding the protection or denial of their rights online—such as free speech, privacy, and safety and security—in selected African countries is examined here as an outcome of constraining or enabling Internet policy and regulatory frameworks. Demand-side survey data are analyzed within the context of the Internet ecosystem as it plays out at the national level in three sub-Saharan African jurisdictions: Nigeria, Rwanda, and South Africa. African Internet users' perception data have been collected through ICT access and use surveys with national representation in 2017.

We begin with an introduction of the main aspects of the African online regulatory systems as they have been identified and discussed by scholars in this field. We then present data on the online experience of Nigerian, Rwandan, and South African users, highlighting their perceived freedom (or lack thereof) when operating online. Findings show that the dynamics of, and experience in, the online environment do have a limiting impact on the user's choices and expression. Last, we briefly contextualize these findings within the framework of the Sustainable Development Goals (SDGs), emphasizing the role that the Internet plays in contributing to a country's growth when relevant policies are formulated in a way that addresses users' needs while safeguarding their rights.

Contextualizing the Online Regulatory System in Africa

Internet use and Internet access from a rights-oriented perspective are understood as the capability to retrieve, produce, and distribute information (text, visual, audio, and video) over the Internet. This translates into freedom of expression, freedom to participate in civic and political activities, freedom to enhance literacy, freedom to improve economic conditions, and freedom to access entertainment and leisure (Rong, 2015). Constraints on Internet use may arise not only from high prices and poor quality of services (Stork, Calandro, & Gillwald, 2013), but also from users' anxiety over restrictive measures that govern the Internet. Such measures may include nontransparent surveillance, content regulation or content filters, more formal limitations on freedom of expression, and retrogressive cybersecurity measures, as well as the absence of these.

Studies on censorship have mostly focused on measuring the technical level of control (Jones & Feamster, 2015) by analyzing DNS (Domain Name System) manipulation (Anderson, Winter, & Roy, 2014; Sfakianakis, Athanasopoulos, & Ioannidis, 2011) with the support of censorship measurement platforms (Crandall, Zinn, Byrd, Barr, & East, 2007; Filastò & Appelbaum, 2012; Sfakianakis et al., 2011). In other words, although measurements for censorship practices do exist, instruments to capture factual experiences about censorship and its resulting impact on Internet users' perception of online freedom have not yet been developed.

The 2017 Freedom House report *Freedom on the Net* has sought to measure the severity of this phenomenon through an examination of social media manipulation to undermine democracy. The research methodology used in the assessment of the level of Internet freedom is based on experts' opinions. Consequently, in an attempt to map efforts to measure censorship, what is missing in the report's findings is the crucial issue of Internet users' perspective on their lack of freedom.

Globally, epistemic communities (Haas, 1992) have developed norms and "best practices" that are introduced to developing countries mostly through capacity building and technical assistance by multilateral organizations (Calandro, 2015a). Yet, democratic assumptions about human rights, freedom of expression, privacy, and security that inform policies and frameworks in the Global North may diverge from those in African countries (Gillwald, 2014). Moreover, on the broader topic of information and communication technology, as Gigler (2015) states,

Existing approaches [to ICTs] have focused too often on issues related to the digital divide and have overemphasized the role of technology itself in addressing these challenges. . . . We need to go beyond the debate about the "digital divide" and instead focus our attention on issues related to the underlying "capability divide." The central issue is, in fact, how poor communities can own, shape, and enact technology based on their own worldviews and derive real economic, social, and political benefits from the use of ICTs. (p. 4)

This goes with the recognition that while access to technology may be available, the undemocratic practices adopted in certain contexts may heavily impact its benefits. Issues around Internet freedom and freedom of expression in African countries need to be contextualized in their own specific political economy and within their own specific Internet ecosystem, which are different from those in the Global North. Although based on similar standards and protocols developed by technical international bodies such as the ICANN (Internet Corporation for Assigned Names and Numbers), the IETF (Internet Engineering Task Force), and the W3C (World Wide Web Consortium)—generally characterized by a limited participation of African stakeholders—the Internet ecosystem as it manifests itself in most African countries carries low levels of access and use of broadband; high prices and poor service quality; lack or underuse of physical resources, such as Internet exchange points; dearth of local content; and an irrelevant number of domain name registrars serving an absent or nascent Internet industry (Calandro, Zingales, & Gillwald, 2013; Chavula, Phokeer, Formoso, & Feamster, 2017; Research ICT Africa, 2017). Also, although the advent of mobile Internet did represent an improvement for Internet access, it also made Internet users (especially those with a lower level of education) more vulnerable to malicious online activities.

Although a globally accepted and ratified human rights framework may be applied as a standard for making Internet policy to address issues such as privacy protection, free flow of information, or freedom of expression (Jørgensen, 2013), the best-practice model based on the Western values of mature democracies often collides with the political economy of fragile African democratic states (Khan, 2002, 2005) and with their underresourced institutional arrangements, which often lack necessary technical skills and financial resources to effectively implement reforms (Gillwald, 2005).

Methodology

The findings presented here are based on nationally representative ICT surveys conducted in 10 African countries in 2017–2018: Ghana, Kenya, Lesotho, Mozambique, Nigeria, Rwanda, Senegal, South Africa, Tanzania, and Uganda. The surveys use enumerator areas (EAs) of national census sample frames as primary sampling units. Using a random sampling technique, in the first stage, the national census sample frames are split into urban and rural EAs. Second, EAs are sampled for each stratum using probability proportional to size. For each EA, two listings are compiled—one for households and one for businesses. The listings serve as sample frames for simple random samplings. A target of 24 households and businesses is sampled for each stratum, using random samples for each selected EA. From the listed household, both residents 15 years of age or older and overnight visitors are randomly selected based on simple random sampling techniques. This methodology provides a good representation across gender, age, and income measures. Survey results are layered with the most recent surveys or national census data in each country to adjust any misbalance with statistical weighting on completion of the survey (Research ICT Africa, 2018).

The analysis that follows focuses specifically on data from Nigeria, South Africa, and Rwanda. The surveys, distributed by a research team led by Research ICT Africa, reached a total of 1,808 respondents in Nigeria, 1,211 in Rwanda, and 1,815 in South Africa. The socioeconomic and political contexts of these countries make them relevant for conducting this type of study in these three jurisdictions, given that all are experiencing political or regulatory limitation to Internet freedom. National policy and regulatory frameworks affecting Internet freedom and the resulting potential restrictions online are also briefly presented.

In Nigeria, which represents one of the biggest markets for digital communications in Africa, the 1999 constitution guarantees freedom of expression and a free press; however, the country's vibrant and active media sector continues to face numerous attempts by state and nonstate actors to suppress political criticism and intimidate journalists into silence (Freedom House, 2015). Rwanda is the top-ranked African country (and the second-ranked overall) among the Low-Income Countries results in the 2017 Affordability Drivers Index, produced yearly by the Alliance for the Affordable Internet (A4AI). According to A4AI (2017), this reflects the success of its "progressive" policies, which have been designed to leverage the ICT sector as an engine for economic and social development. Although there is no doubt that Rwanda has made impressive progress in economic and social development since the 1994 genocide, it is equally true that the government imposes severe restrictions on freedom of expression and does not tolerate dissent (Human Rights Watch, 2016).

South Africa has the highest level of Internet access and use across all countries under investigation (Research ICT Africa, 2017). Despite Internet access in South Africa remaining free and open, two legislative proposals may limit Internet freedom in the country. Legislation passed by Parliament at the beginning of 2018, which aims to protect children online, has the potential to impose "censorship by proxy" by ruling that social media platforms must classify all digital information they want to provide before it is published online (Calandro, 2015b). In addition, the adoption of the Cybercrime and Cybersecurity Bill, which from 2018 has been amended into the Cybercrime Bill, played a potentially alarming role in relation to the

constitutional right to free speech because its definition of hate speech was broader than the one contained in the Constitution (Research ICT Africa, 2015).

The following analysis compares Nigeria, Rwanda, and South Africa, three of the countries covered by the #AfterAccess Surveys conducted in 2017. The data presented next offer an overview of the users' personal experience with communication technology, and the subsequent discussion unpacks more specific issues related to their perception of online freedom.

Results

The advancement in the telecommunications industry in sub-Saharan Africa, driven by the reduction in the price of equipment, devices, and data bandwidth, has increased mobile phone penetration, with about 7 of 10 people residing in the After Access-surveyed countries owning a mobile device. Although this indicator is positive, smartphone proliferation has not increased at the same pace, and Internet use in sub-Saharan Africa has remained below average in comparison with other continents (International Telecommunication Union, 2018). The After Access Survey findings indicate that Internet penetration is highly aligned with smartphone penetration. Among the surveyed countries, South Africa, which has the highest GNI per capita among the countries surveyed, is the only one with slightly more than 50% of its population using the Internet—a number aligned with smartphone penetration in the country. In contrast, Rwanda has the lowest smartphone penetration, at 9%. Despite Nigeria being classified as the largest economy in Africa, smartphone penetration in the country (23%) is considerably lower than in South Africa (Gillwald & Mothobi, 2018).

In relation to mobile phone ownership (see Table 1), a breach in privacy does not appear to be of concern in South Africa. Even in Rwanda, only 4.38% of mobile phone nonowners have privacy concerns, while in Nigeria, the percentage is slightly higher (6.14%).

Table 1. Main Reasons for Not Owning a Mobile Phone.

	Nigeria (%)	Rwanda (%)	South Africa (%)
I cannot afford it	56.16	66.13	42.68
No mobile coverage	20.71	11.30	0.63
No electricity at home to charge the phone	26.54	50.87	0.55
My phone is broken	15.08	10.31	24.48
My phone got stolen	11.89	8.08	14.72
I don't know how to use it	18.70		11.86
I don't need it	19.09		
I am not allowed to own one	11.74	15.03	8.66
I have privacy concerns	6.14	4.38	1.25

Source. After Access Survey within the Research ICT Africa, 2017 Research ICT Africa, 2017.

When it comes to limitations in Internet use (presented in Table 2), in Rwanda, according to 8.49% of Internet users, lack of content in local languages is a barrier.

Table 2. Internet Users' Main Reasons for Not Using the Internet.

	Nigeria (%)	Rwanda (%)	South Africa (%)
Nothing, no limitation	18.26	21.58	
Lack of time	16.16	18.13	
Data cost	32.85	48.7	
Lack of content in my language	0.27	8.49	3.32
Speed of Internet	17.35	1.01	
Privacy concerns	2.94	2.08	
Worried about getting virus/malware		9.97	3.77
Not allowed to use it more (family limits Internet use)	1.1	2.95	2.88
Find it difficult to use	1.57		
No interesting content for me		9.1	7.8
Internet is very slow		19.08	24.22
Internet is too expensive		55.95	47.15
Few people to communicate with via the Internet		23.47	5.73
Worried about surveillance/privacy invasion		7.78	3.18

Source. After Access Survey within the Research ICT Africa, 2017 Research ICT Africa, 2017.

Also, 1 of 10 Internet users (9.97%) is concerned about the danger of viruses or malware affecting their device. In South Africa, 7.8% of Internet users do not seem to find content that is of interest to them, while Nigerians are not overly impacted by a lack of content in local languages.

Table 3 shows that for the Internet nonusers, similar to the Internet users, factors such as lack of content in local languages or privacy invasions are not listed among the main barriers to accessing the Internet.

Table 3. Internet Nonusers' Main Reasons for Not Using the Internet.

	Nigeria (%)	Rwanda (%)	South Africa (%)
I don't know what the Internet is	39.63	8.86	36.18
No access to device (computer/smartphone)	13.41	42.82	15.67
No interest/not useful	9.96	3.82	9.05
I don't know how to use it	21.98	2.69	2.74
Not available in my area	4.2		14.99
Too expensive	4.02	32.97	14.99
No time, too busy	3.33	3.97	8.6
None of my friends use it	0.28		0.29
Lack of content in my language	0.35	0.69	0.54
Worried about privacy invasion	0.27		0.47
My spouse or parents do not allow me to use it	1.26	0.27	4.58
Other	1.31		6.89

Source. After Access Survey within the Research ICT Africa, 2017 Research ICT Africa, 2017.

With regard to social media use—according to Stork et al. (2013), one of the main reasons that people use the Internet in Africa—the majority of users are not concerned about sharing their real names online. On the other hand, personal details, such as marital status, mobile number/e-mail, and pictures are not shared by 50% of Internet users in South Africa. Moreover, only a small portion of Internet users in the country share their spiritual faith (28.11%), and even fewer share their political views (11.1%) and sexual orientation (11.15%). Similarly, in Rwanda, half of Internet users do not share their mobile number or email address on social media. In Nigeria, the majority of Internet users tend not to share their personal information, except for their political views (shared by only 23.35% of Internet users) and their sexual orientation (21.58%). These data are reported in Table 4.

Table 4. Information Shared on Social Media.

	Nigeria (%)	Rwanda (%)	South Africa (%)
Real name	89.75	90.4	73.27
Gender	98.57	89.86	62.65
Age	75.76	78.79	56.05
Marital status	84.91	82.91	46.32
Mobile number/e-mail	80.02	53.44	36.45
Your or your family's and friends' pictures and videos	86.96	84.55	53.01
Religion	79	64.81	28.11
Political views	42.92	23.78	11.1
Sexual orientation	21.58	28.35	11.15

Source. After Access Survey within the Research ICT Africa, 2017 Research ICT Africa, 2017.

In relation to their openness in discussing certain topics on social media, Internet users show different feelings (see Table 5). The majority of users across all countries under investigation do not feel comfortable openly discussing gossip on social media, and only a minority (less than 10%) feel comfortable gossiping publicly. Internet users feel more comfortable discussing professional and work-related matters, but mostly in closed groups. Overall, in South Africa (57.65%), Rwanda (44.22%), and Nigeria (44.29%), the majority of Internet users do not feel comfortable at all discussing professional issues. Conversely, the majority of Nigerian users feel comfortable talking about issues of a religious nature (41,1%), which is in sharp contrast to South African and Rwandan users, who prefer not to discuss religious matters on social media (56.66% and 44.67%, respectively).

On average, across all countries under investigation, financial information is the most sensitive topic. As shown again in Table 5, the majority of Internet users across the board do not feel comfortable discussing financial information on social media. Similarly, there appears to be a preference for not sharing political matters, or at least doing so in closed groups (14.49% in Nigeria, 17.03% in Rwanda, and 15.07% in South Africa). There is also a preference for keeping health and sexual matters private, although a higher number of Internet users (25.53% in Nigeria, 22.96% in Rwanda, and 19.29% in South Africa) feel comfortable discussing these issues in closed groups.

Table 5. Degree of Comfort Discussing Specific Topics.

		Nigeria (%)	Rwanda (%)	South Africa (%)
Gossip	Not at all	50.25	43.07	57.2
	Yes, but only in closed groups	39.73	51.12	36.13
	Yes, publicly	10.03	5.81	6.67
Professional/work related-matters	Not at all	44.29	44.22	57.65
	Yes, but only in closed groups	35.39	43.11	30.4
	Yes, publicly	20.32	12.67	11.95
Religious matters	Not at all	34.15	44.67	56.66
	Yes, but only in closed groups	24.74	33.39	24.23
	Yes, publicly	41.1	21.94	19.11
Political matters	Not at all	59.19	75.77	75.96
	Yes, but only in closed groups	14.49	17.03	15.07
	Yes, publicly	26.31	7.19	8.96
Financial information	Not at all	68.17	72.05	79.91
	Yes, but only in closed groups	20.14	16.69	16.1
	Yes, publicly	11.69	11.26	3.98
Health and sexual matters	Not at all	57.64	73.63	75.21
	Yes, but only in closed groups	25.53	22.96	19.29
	Yes, publicly	16.84	3.41	5.5

Source. After Access Survey within the Research ICT Africa, 2017 Research ICT Africa, 2017.

Freedom of expression can at times have negative consequences, especially if the opinion that is freely expressed causes damage or trauma to somebody else. To avoid such consequences, constitutional limitations are in place in relation to what can be freely expressed and what is forbidden because of its potential to cause harm. Nevertheless, on social media, because of lack of awareness, limited media literacy, or even a perception of freedom that goes beyond constitutional limits given its "online" form, users may have used these platforms to harm others.

As evidenced by the data presented in Table 6, in the sub-Saharan African countries under investigation, less than 15% of Internet users of 15 years of age or older have been victims of cyberbullying. In South Africa, more specifically, only 3.93% seem to have ever experienced cyberbullying. The percentage is higher in Nigeria and Rwanda, where 12.53% and 14.23% of users, respectively, have encountered cyberbullying. At the same time, however, a higher proportion of Internet users have been recipients of unwanted or offensive content, for a number of possible reasons. First, the majority of victims of cyberbullying may be users younger than 15 years of age. Second, in some cases, the intention of the sender may be misunderstood by the recipient, and an image or a sentence intended to be amusing by the sender might be perceived as offensive by the receiver. Because of religious, cultural, or gender differences, different users might perceive what represents offensive content in different ways. Finally, in other cases, an image or content can be sent with the specific intention of offending the recipient. This issue seems to be particularly problematic in Rwanda, where one out of five users has been confronted with unwanted or offensive content.

Table 6. Percentage of Internet Users (15 years +) Who Have Been Victims of Cyberbullying or Exposed to Offensive Content.

	Nigeria (%)	Rwanda (%)	South Africa (%)
Have you ever been a victim of cyberbullying?	12.53	14.23	3.93
Were you ever confronted with unwanted or offensive content?	17.97	21.35	13.79

Source. After Access Survey within the Research ICT Africa, 2017 Research ICT Africa, 2017.

In relation to perceived safety and security online, which has been assessed through Internet users' experience of account hijacking or online fraud (see Table 7), 6.14% and 6.81% of Internet users in Nigeria and South Africa, respectively, have been conned over the Internet and lost money. With reference to account hacking, less than 10% of Internet users have been victims of this cybercrime,² with more of those affected located in Nigeria rather than in South Africa.

Table 7: Internet Users' Experience of Cybercrime.

	Nigeria (%)	South Africa (%)
Have you ever been conned over the Internet and lost money?	6.14	6.81
Has your e-mail account ever been hacked and hijacked?	5.72	4.03
Has your social media account ever been hacked or hijacked?	7.21	4.36

Source. After Access Survey within the Research ICT Africa, 2017 Research ICT Africa, 2017.

Discussion

On balance, across all the countries under investigation, privacy concerns and lack of content in local languages do not appear to be the main aspects hindering access to the Internet. As of 2017, the more pressing issue of broadband affordability is still the main obstacle to a seamless network experience. Overall, the Internet is also not perceived as an unsafe environment, given that only a small number of users have experienced cyberbullying or have been confronted with unwanted digital content. Nevertheless, survey results show that a percentage of Internet users in both Nigeria and South Africa have incurred in financial loss through online fraud, and in Nigeria, social media users have had their accounts hacked.

In terms of Internet freedom, those with regular online access and use of social media have put in place different measures of self-protection in the way they share personal information. Not only do the majority of social media users in South Africa, Nigeria, and Rwanda prefer not to share specific personal details, but they also tend not to discuss business, health/sexual matters, and political topics with public online networks. When discussions on these topics do occur, they usually take place within smaller and trusted groups.

While the investigation of the reasons behind such forms of self-imposed content control is beyond the scope of this research, the descriptive statistics on Internet users' experience of online freedom

² Cybercrime is defined in the literature as any crime committed both against data and computer systems and by means of computer systems. Fighting cybercrime is only one of the key policy areas contributing to cybersecurity broadly defined (Porcedda, 2014).

presented here reveal, overall, that the majority of African users do not trust that portion of social media that is publicly accessible. Yet, this does not seem to derive from privacy or cybersecurity concerns, given that less than 5% of Internet users consider invasion of privacy to be a problem of Internet use (see Table 2), less than 8% have experienced cybercrime (see Table 7), and less than 15% have ever experienced cyberbullying (see Table 6).

The resource-constrained settings of sub-Saharan Africa, characterized by little awareness of cybersecurity risks and privacy violations, may impact security decisions from a user perspective. Awareness of the harms associated with cybercrime has resulted in the adoption, by several governments, of international technical standards for cybersecurity and in the establishment of different forms of computer emergency response teams (CERTs). Yet, a technical and narrow approach to institutions, processes, and rules in this area, which are outside a human rights and good governance framework, may have the unintended outcome of effectively weakening the protection of individual rights.

Assessing the appropriate role for the state in cyberspace governance and the institutional arrangements that arise from it is one of the primary policy challenges facing developing countries. States are critical in reducing vulnerability to shocks, and effective state-led measures can guarantee security and the rule of law; they can also facilitate the design and implementation of effective strategies to ensure the development of legal frameworks for a safe and secure cyberspace. Although development theory is based on a commitment to freedom, equity, and cooperative interdependence, a necessary part of supporting development processes must include holding states accountable regarding their commitment to the Universal Declaration of Human Rights as a global governance standard. Hence, a rights-based approach should be at the core of an open Internet. An additional challenge in development is therefore that of building states that not only are accountable and able to tackle poverty and inequality, but also can protect the rights of their citizens—including the right to be safe and free online.

Policy Implications Within the Sustainable Development Goals Framework

Leading organizations in the area of Internet policy analysis have been advocating the crucial role that ICT plays in contributing to a country's development and, more specifically, in achieving the SDGs. Researchers at the Earth Institute of Colombia University (2017), for example, have recognized ICT's power to bring about a digital transformation of society as a whole. Specifically, it has extraordinary

potential to increase the rate of diffusion of a very wide range of technologies across the economy. . . . The accelerated uptake of these technologies and others empowered by ICTs constitute the key to achieving the Sustainable Development Goals by their target date of 2030. (p. 12)

At the same time, as the Internet Society (2015a) highlights, it is necessary to not only build a realistic understanding of how the Internet, specifically, can contribute toward the SDGs at a global, national, and local scale, but also identify the constraints that must be overcome. This has a direct relation to the way citizens perceive the protection of their freedom online and choose to engage with ICTs.

The goal of *ending poverty in all its forms* placed at the center of SDG 1 means that, besides the provision of accurate information, ICT is vital in enabling mobile banking and micro-credit services (Columbia University, 2017). Hence, the online environment of Internet-enabled services for e-government and e-business must be regulated in a way that makes transactions and interactions safe for individuals and businesses to feel confident in their use; facilitating cybersecurity in this area is essential (Internet Society, 2015a). As the Internet Society (2015b) expounds,

A security paradigm for the Internet should be premised on fostering confidence and protecting opportunities for economic and social prosperity, as opposed to a model that is based simply on preventing perceived harm. Moreover, security solutions should advance that objective in design, and in practice. Otherwise, security solutions may go too far, thereby jeopardizing the very infrastructure that ties together the global economy, and provides the engine for its growth. (p. 2)

On a similar course of action, SDG 10's focus on *reducing inequalities* calls for an approach to ICT that sees technologies being used with the purpose of bringing information and knowledge to more disadvantaged groups in society, facilitating all-encompassing social and economic progress (Columbia University, 2017). In relation to *peace, justice, and strong institutions*, the focus of SDG 16, governments' use of open data offers increased transparency and empowers citizens by allowing them to make critical choices for their lives, which indirectly support economic growth (Columbia University, 2017). This, again, calls for a collaborative security approach that builds trust in online services, ensures that data are secure, and makes the use of networks and services reliable. This is particularly important when dealing with health or financial transfers (Internet Society, 2015a). At the same time, citizens' ability to express themselves freely online is a centerpiece for political rights and civil liberties, which are fundamental elements in the context of SDG 16 (Garrido, Fellows, & Koepke, 2017).

Recognizing the importance of the connection between Internet freedom, online engagement and development is essential to create an environment in which people feel free and safe to engage with ICTs. A regulatory framework that enables such an environment is one that allows a country to develop innovatively by capitalizing on both current and emerging online technologies.

Conclusions

Internet freedom emerges as a development issue when retrogressive online and offline information, as well as content regulation, can have profound implications for individuals' capabilities. From a policy perspective, beyond the more obvious negative impact of retrogressive Internet regulation on users' civil and political rights, there is a need to understand unintended consequences in terms of reducing Internet use as a result of content regulation, and the linkages of Internet policy and regulation within national polities. In particular, to protect Internet users, we need to better understand, on the one hand, what the risks of using the Internet are, and on the other hand, how emerging forms of Internet regulation may impact Internet use and access beyond the well-known negative effects of high prices and poor quality of broadband services in low- and middle-income countries. This must be assessed to protect Internet users and to develop both technological and advocacy measures that address real and concrete threats.

The discussion presented in this article through the analysis of demand-side survey data from Nigeria, Rwanda, and South Africa examined within the context of the African Internet ecosystem shows that while users do not fear access to cyberspace, the negative experiences they (or those they know) have experienced online, either through fraud or personal information hacking, have limited their freedom of speech on particular topics. Even when self-imposed, such restrictions may have broader repercussions on development and growth in the long term, and in relation to the targets that countries have set for their endeavors toward the achievement of the SDGs.

The importance of formulating cybersecurity measures that allow users to feel safe online is unquestioned. Yet, policies in this area must also be created with citizens' rights in mind. As the Internet Society (2015b) states, "Security solutions should be fully integrated with . . . fundamental human rights, values, and expectations (e.g., privacy, freedom of expression)" (p. 3). Ensuring that Internet users can operate in an online environment that is free from threats and facilitates open interaction and communication, including service-related transactions, is a crucial point in the development agenda of governments in middle- and low-income countries. Further research that is helpful in increasing knowledge about African users' perception of their freedom online can contribute to the development of policies that address both the threats experienced by users and the perceived and real obstacles that limit their ability to express themselves freely.

References

- Abdulrauf, L. A. (2018). The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa. *African Human Rights Law Journal*, 18(1), 365–391. doi:10.17159/1996-2096/2018/v18n1a17
- A4AI. (2017). *2017 Affordability report*. Washington DC: Author. <http://1e8q3q16vyc81g8l3h3md6q5f5e-wpengine.netdna-ssl.com/wp-content/uploads/2017/02/A4AI-2017-Affordability-Report.pdf>
- Anderson, C., Winter, P., & Roy, F. (2014, August). *Global network interference detection over the RIPE Atlas network*. Paper presented at the 4th USENIX Workshop on Free and Open Communications the Internet (FOCI 14), San Diego, CA.
- Bitso, C. (2014). Internet censorship in South Africa: A brief exposé of negative and positive trends. *South African Journal of Libraries and Information Science*, 80(1), 41–51. <https://doi.org/10.7553/80-1-1388>
- Calandro, E. (2015a). *Governing regional telecommunication networks in a developing region: The SADC case* (Unpublished doctoral dissertation). University of Cape Town, South Africa. <https://open.uct.ac.za/handle/11427/16431>

- Calandro, E. (2015b). *The South African draft online regulation policy as a form of "censorship by proxy."* Cape Town, South Africa: Research ICT Africa. <https://researchictafrica.net/2015/05/29/the-south-african-draft-online-regulation-policy-as-a-form-of-censorship-by-proxy/>
- Calandro, E., Zingales, N., & Gillwald, A. (2013). *Mapping multistakeholderism in Internet governance—Implications for Africa* (Discussion paper). Cape Town, South Africa: Research ICT Africa.
- Chavula, J., Phokeer, A., Formoso, A., & Feamster, N. (2017, September). *Insight into Africa's country-level latencies*. Paper presented at the Institute of Electrical and Electronics Engineering (IEEE) AFRICON Conference, Cape Town, South Africa. https://www.researchgate.net/publication/321353348_Insight_into_Africa%27s_country-level_latencies
- Columbia University. (2017). *ICTs & SDGs: How information and communication technology can accelerate action on the sustainable development goals*. New York, NY: The Earth Institute, Columbia University. <https://www.oneworld.net/sites/default/files/resources/2016-06/ict-sdg.pdf>
- Crandall, J., Zinn, D., Byrd, M., Barr, E., & East, R. (2007, November). Concept doppler: A weather tracker for Internet censorship. In *CCS '07a: Proceedings of the 14th ACM Conference on Computer and Communications Security* (pp. 352–365). New York, NY: Association for Computing Machinery (ACM).
- Filastò, A., & Appelbaum, J. (2012, August). *OONI: Open Observatory of Network Interference*. Paper presented at the 2nd USENIX Workshop on Free and Open Communications on the Internet, Bellevue, WA.
- Freedom House. (2017). *Freedom on the Net. Manipulating social media to undermine democracy*. Washington DC: Author. https://freedomhouse.org/sites/default/files/2020-02/FOTN_2017_Final_compressed.pdf
- Garrido, M., Fellows, M., & Koepke, L. (2017). The state of access to information and development in the United Nations 2030 Agenda. In M. Garrido & S. Wyber (Eds.), *Development and access to information* (pp. 15–49). The Hague, The Netherlands: International Federation of Library Associations and Institutions (IFLA). <https://www.db.dk/files/Development%20and%20Access%20to%20Information%202017%20-%20da2i-2017-full-report%20IFLA.pdf>
- Gigler, B. S. (2015). *Development as freedom in a digital age*. Washington, DC: World Bank.
- Gillwald, A. (2005). *Toward an African e-index: Household and individual ICT access and usage in 10 African countries*. Johannesburg, South Africa: The Link Centre.
- Gillwald, A. (2014). *Comments for Stockholm Internet Forum (SIF14)*. Cape Town, South Africa: Research ICT Africa. <https://researchictafrica.net/2015/05/29/comments-for-stockholm-internet-forum-sif14-by-alison-gillwald/>

- Gillwald, A., & Mothobi, O. (2018). *After Access 2018: A demand-side view of mobile Internet from 10 African countries*. Cape Town, South Africa: Research ICT Africa. https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access_Africa-Comparative-report.pdf
- Haas, P. E. (1992). Introduction: Epistemic communities and international policy coordination. *International Organization*, 46(1), 1–35. doi:10.1017/S0020818300001442
- Human Rights Watch. (2016). *World Report 2016*. <https://www.hrw.org/world-report/2016>
- International Telecommunication Union. (2018). *Measuring the Information Society Report* (Vol. 1). Geneva, Switzerland: Author. <https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf>
- Internet Society. (2015a). *The Internet and sustainable development: An Internet Society contribution to the United Nations discussion on the Sustainable Development Goals and on the 10-year review of the World Summit on the Information Society*. Geneva, Switzerland: Author. <https://www.internetsociety.org/wp-content/uploads/2015/06/ISOC-ICTs-SDGs-201506-Final.pdf>
- Internet Society. (2015b). *Collaborative security: An approach to tackling Internet security issues*. Geneva, Switzerland: Author. <https://www.internetsociety.org/wp-content/uploads/2015/04/Collaborative-Security.pdf>
- Jones, B., & Feamster, N. (2015, August). *Can censorship measurements be safe(r)?* Paper presented at ACM Special Interest Group on Data Communication (SIGCOMM) Conference, London, UK.
- Jørgensen, R. F. (2013). An Internet bill of rights? In I. Brown (Ed.), *Research handbook on governance of the Internet* (pp. 352–372). Cheltenham, UK: Edward Elgar.
- Khan, M. H. (2002). State failure in developing countries and strategies of institutional reform. In B. Tungodden, N. Ster, & I. Kolstad (Eds.), *Toward pro-poor policies, aid, institutions, and globalization: Annual World Bank Conference on development economics, Europe (2003)* (pp. 165–195). Oxford, UK: Oxford University Press and World Bank.
- Khan, M. H. (2005). Markets, states and democracy: Patron-client networks and the case for democracy in developing countries. In J. Faundez (Ed.), *Special issues of democratization: On the state of democracy*. London, UK: SOAS, University of London. http://www.networkideas.org/featart/feb2007/Markets_States_Democracy.pdf
- Lumbu, R. N. (2018). *Compendium on the legal protection of human rights defenders in Africa*. Pretoria, South Africa: Pretoria University Law Press.
- Porcedda, M. C. (2014). Rule of law and human rights in cyberspace. In P. Pawlak (Ed.), *Riding the digital wave: The impact of cyber capacity building on human development* (pp. 28–42). Paris, France:

- European Union Institute for Security Studies*. https://www.files.ethz.ch/isn/186860/Report_21_Cyber.pdf
- Research ICT Africa. (2015). *Submission on the Cybercrime and Cybersecurity Bill*. Cape Town, South Africa: Author. https://www.researchictafrica.net/publications/Other_publications/2015_RIA_Submission_to_Cybersecurity_and_Cybercrime_Draft_Bill.pdf
- Research ICT Africa. (2017). "One size fits all" mobile and Internet policies Global South. Cape Town, South Africa: Author. <https://afteraccess.net/the-inside-internet-story-of-africa>
- Research ICT Africa. (2018). *ICT HH and business survey field manual*. Cape Town, South Africa: Author. <https://researchictafrica.net/wp/wp-content/uploads/2018/04/2018-HH-Survey-Training-Manual-1.pdf>
- Rong, W. (2015). Internet use and the building of social capital for development: A network perspective. *Information Technologies & International Development Journal*, 11(2), 19–34.
- Sfakianakis, A., Athanasopoulos, E., & Ioannidis, S. (2011, August). *CensMon: A Web censorship monitor*. Paper presented at the 1st USENIX Workshop on Free and Open Communications on the Internet (FOCI 11), San Diego, CA.
- Stork, C., Calandro, E., & Gillwald, A. (2013). Internet going mobile: Internet access and use in 11 African countries. *Info*, 15(5), 34–51. doi:10.1108/info-05-2013-0026
- Turianskyi, K. (2018). *Balancing cyber security and Internet freedom in Africa* (South African Institute of International Affairs Occasional Paper 275). Johannesburg, South Africa: South African Institute of International Affairs. https://media.africaportal.org/documents/OP_275_GAP_Turianskyi_FINAL_WEB.pdf