WHEN GOVERNMENTS DEFRIEND SOCIAL MEDIA

A study of Internet-based information controls in the Kingdom of Lesotho with a particular focus on the period around the 3 June 2017 General Elections

Arthur Gwagwa
Senior Research Fellow

Centre for Intellectual Property and Information Technology Law, Strathmore Law School
Strathmore University, Nairobi, Kenya

Funded by the Open Technology Fund

30 June 2017

Table of Contents

KEY FINDINGS

The Lesotho government maintained a hostile stance towards social media, and attempted to shut it down twice during the election period. It sought to take this measure in response to an increase in the use of social media and online publishing platforms. Technical network measurements we carried out during the election period did not reveal clear evidence that the government had successfully blocked website pages. This could be attributed to three main factors. Firstly, Lesotho has very few standalone websites providing local content, and it is difficult for the government to filter or block the more commonly-used websites. Secondly, the government lacked the technical capabilities to shut down the internet or social media. Finally, the Lesotho Communications Authority resisted a government directive to shut down social media, insisting on due process and the need to respect freedom of expression. Given that the government has previously censored and shut down print and broadcast media, it is highly likely that it would have shut down social media if it had the capacity to do so, and if the regulator had complied with its directive.

The current government, which came into power on 3 June 2017, has not announced its plans on internet policy and social media. However, at a policy level, Lesotho has been slowly working on data protection and cybersecurity legislative frameworks since 2012. Once operational, the data protection legislation will introduce progressive provisions to protect usage of private data. Similarly, the pending computer crime and electronic transactions bills include progressive provisions, including measures to protect intermediaries within Internet ecosystems from liability for third party content.

The universal service fund investment has extended 3G and 4G mobile network reach, which has increased the use of social media and internet-based radio stations, and had a catalytic effect on freedom of expression and the opening up of political space. However, alongside these infrastructural developments there is a need to mainstream an understanding of human rights in cybersecurity. While the Regulator has often factored human rights considerations into its decision making, other stakeholders, such as law enforcement branches and the government, require further training and political will to apply human rights and the principles that underpin them, such as the need for transparent and inclusive decision making.

I. INTRODUCTION

Political Context

This report follows my visit to Maseru, the capital city of Lesotho, from 29 May to 6 June 2017, where I monitored the exercise of human rights on the internet during the country's general elections on 3 June 2017. The scheduled elections determined all 120 seats of the National Assembly; the lower house of the Parliament. They were called more than three years ahead of schedule due to a successful vote of no confidence against the incumbent Prime Minister, Pakalitha Mosisili of the Democratic Congress (DC) party. Thomas Motsoahae "Tom" Thabane, of the All Basotho Convention (ABC) party, defeated Mosisili and was sworn in as Prime Minister on 16 June. Although the elections occurred under peaceful conditions, Tom Thabane›s estranged wife Dipolelo was shot and killed on 14 June.[1] This again called into question the country's commitment to ending the culture of extra-judicial killings and impunity.

Methodology

We performed limited Open Observatory of Network Interference to examine whether websites were blocked during the general election. The raw data is accessible by clicking the following link: https://measurements.ooni.torproject.org/files/by_country/LS.[2] We also examined internet activities in the country ahead of and during the elections, using various data science baseline projects such as Shodan and RIPE ATLAS probes.

In addition, we met with various stakeholders, including senior officials in the Lesotho Communications Authority (the "Regulator"), and with political and civil society leaders working on freedom of expression, including in the digital context. Prior to this, we carried out background research and preparatory work that included issue- and stakeholder-scoping, for example during my meeting at the Open Society Institute of Southern Africa (OSISA) offices in Johannesburg, South Africa.

In examining whether the government and other non-state actors are restricting internet resources and content, the report examines the following issues:

- restriction of content on the Internet including arbitrary blocking, throttling or filtering of content, and criminalization of legitimate expression including the imposition of intermediary liability and cyber-attacks;
- inadequate protection of the right to privacy and data protection as well as an understanding and application of cybersecurity policies, and;
- access to the internet and the necessary infrastructure, including usage of the universal service fund.

Finally, it considers what efforts government, the Regulator, private sector and civil society are applying to address presenting issues, such as the extent to which the Regulator may be pushing back against executive powers.

[1] 'Killing' of Lesotho PM Thabane›s wife raises instability fears: http://m.news24.com/news24/Africa/News/killing-of-lesotho-pm-thabanes-wife-raises-instability-fears-20170615

[2] A crucial aspect of the research is running OONI software tests. The Open Observatory of Network Interference (https://ooni.torproject.org/), a free software project that aims to increase transparency around internet censorship through the collection of network measurements. In particular, it runs numerous software tests (called ooniprobe) that are designed to examine blocking of websites, WhatsApp, Facebook Messenger, and Telegram etc.

Rationale for the Study

The project arises from a realisation that Internet shutdowns, disruptions and other forms of censorship, carried out to stifle communications amongst protesters and impede dissenting views, are increasingly common in African countries during election periods. According to a recent report by the New America Foundation, in addition to an already diverse portfolio of techniques, governments are increasingly engaging in the complete shutdown of the internet or telecommunication services within their borders.[3] 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.[4]

As more African governments place onerous restrictions to prevent the free flow of information, and directly contradict widely accepted international commitments to human rights such as the Universal Declaration of Human Rights, there is an even greater need for private actors to play a role in upholding the rule of law. Private actors such as telecommunications companies, internet service providers, social media platforms, and Internet Service Providers that are active in the country, working with international bodies such as the U.N., are best served if they act collectively and transparently. When a state gives the instruction to take down a post online or to block a certain website, the various stakeholders need to push back in order to defend human rights norms.[5]

In this report, we summarize some of our key findings pertaining to information controls/internet freedoms in Lesotho, with a particular emphasis on the period in the run up to the elections. We provide an overview of the assortment of approaches the government of Lesotho employed in its attempt to muzzle freedom of expression online, how the Regulator in turn responded in accordance with the rule of law, how such a response helped to protect and promote internet freedom in the country, and the impact of these activities on the outcome of the 2017 general elections.

II. FINDINGS

Social Media Shutdown Attempts

In July 2016, Pakalitha Mosisili's Democratic Congress (DC) Government (the "Government") proposed to close down social media as it felt social media sites were publishing government secrets without consent. In response, the Lesotho Communications Authority (the "Regulator") rejected the proposal and instead asked the Government to give it reasons for its request.[6] In pursuit of its goal, in early November 2016, the Government requested that the Regulator send a written request to the country's two mobile phone carriers and internet providers (Econet and Vodacom) to provide information on whether a temporary restriction of access to Facebook and Twitter usage was possible.

The Media Institute of Southern Africa in Lesotho and the Consumer Protection Agency expressed serious concern about the possible implications of such a request. In response to the request, the Regulator "pushed back" by telling the government that, "Shutting down one platform won't stop political

[3] https://www.newamerica.org/oti/policy-papers/ensuring-future-detecting-internet-disruptions/

[4] For example, the 6 month shut down in the western English speaking portion of Cameroon targeted and specific to stifle dissent.

[5] "What can the UN do if your country cuts the internet" http://www.aljazeera.com/indepth/features/2017/05/country-cuts-internet-170504064432840.html

[6] Regulator Informant

discussions taking place on other platforms"[7]. However, the Government went ahead and sent a letter to the telecommunications providers, stating its own views that rationalised its intention to shut down social media and asking the telecommunications providers for their views on the issue. The operators then intentionally leaked the letters to the community, ostensibly as they feared losing business if such shutdowns were to occur.

The Regulator subsequently invited Facebook to meet government officials and the Regulator to explain why it was important to keep social media and indeed the internet open, because as it turned out, the government did not understand what Facebook was, let alone its important role in society.

In our view, the above scenario demonstrates how diverse stakeholders, in this case, the Regulator, domestic operators and international operators, can work together and with the public to push back against internet shutdowns. Here, by leaking the memorandum, the operators increased transparency and public accountability on the issue which helped to put the government under pressure. According to the regulator: "The minister at the time even ended up not wanting to be associated with the instruction letter when addressing the issue to the media." Also, the Regulator played a crucial role, for example, in its memoranda to the public published on 14 November 2016, it stated that: "Best practices dictate that regulatory process should be followed......The Authority respects freedom of expression in all its forms." In our limited interpretation, both the economic impact and rule of law arguments helped keep the internet open in Lesotho.

A lack of transparency on Cyberspace Governance

The Lesotho previous government's attempt to shutdown social media stems from its culture of excessive secrecy, which in turn is motivated by paranoia and the Internet's prospective capabilities. The government feared the power of the internet to bring about democratic change. For instance, a government employee whose name has been withheld on anonymity grounds stated, "At one point, I was working on minutes for the army and intelligence, and they wanted me to omit some of the proceedings for people not to know what was happening but I responded that 'This isn't supposed to be a secret'".

The same employee also spoke of an instance when, at one point, the army instructed the Regulator to tell Google not to show its barracks on the Google maps. The Regulator responded by telling the army that the maps show nothing other than a mass of land with moving objects.

Paranoia as a basis for policy and government practice is shared among repressive Southern African Governments. In Zimbabwe, Nelson Chamisa, an opposition parliamentarian said that because of their fear of technology, government officials were in support of restrictive legislation on Information and Communication Technologies (ICTs) as a way of safeguarding their personal security while pretending to be in favour of national security.[8] A similar sentiment emerged in an interview with Charles Bradley of the Global Partners' Initiative titled "Are We Missing the Bigger Picture behind Network Disruptions?"[9] In Malawi, the newly passed Electronic Transactions and Cyber Security Act 2017 criminalises "the act of knowingly receiving and sharing unauthorized data" and "wilfully and repeatedly use electronic communication to attempt to disturb the peace or right of privacy of any person".[10] Similarly, in Angola, on June 20, 2017, the government accused

[7] Government employee (name anonymised)

[8] Remarks at an Online Indaba organised by the Media Institute of Southern Africa (MISA) Zimbabwe Chapter in the capital: http://www.thezimbabwean.co/2015/12/technophobic-officials-in-govt/

[9] https://www.gp-digital.org/multimedia/in-beta-episode-4-are-we-missing-the-bigger-picture-behind-network-disruptions/

[10] Malawi tightens grip on Internet usage: http://aa.com.tr/en/africa/malawi-tightens-grip-on-internet-usage/845555

investigative Angolan journalist and Director of the anti-corruption organization Maka Angola, Rafael Marques de Morais, of "outrage to a body of sovereignty and injury against public authority." The accusations stem from Marques's Maka Angola article, in which he exposed Angolan Attorney General João Maria Moreira de Sousa's illegal purchase and sale of state-owned land for personal profit.[11] The indictment states that as the publisher of Maka Angola, Marques is responsible for the article that allegedly violated Angolan state security despite the fact that the Constitution explicitly prohibits the Attorney General from engaging in other professional activities. Commentators have seen this as an abuse of the doctrine of information security to cover up impunity.[12]

A culture of secrecy, including in the digital context, is the antithesis to an open government and demonstrates that one of the most persistent challenges of national security policy is balancing the short-term benefits of secrecy with the long-term benefits of openness. Remarks made by Ron Wyden and John Dickas, albeit in the U.S context, apply:

> "Government officials who ignore this fact and insist on secrecy whenever it seems convenient will serve their agencies and their country poorly."[13]

In the case of Lesotho, just like some other Southern African countries, secrecy on cybersecurity issues can be attributed to a lack of laws, and where they exist, a lack of political will to enforce them.

In August 2013, Resident Magistrate Adv. Motlatsi Petrose Kolisang and Hon. Member of Parliament Adv. Lineo Irene Molise-Mabusela made the following remarks:

> "For a long time, the country of Lesotho had no laws on cybercrimes. However, the country has taken positive steps in an attempt to prevent, control and punish...these crimes. The following law regimes are in the pipeline and are at the verge of enactment into laws. They are: Data Protection Bill 2013, Computer Crime and Cybercrime Bill 2013 and Lesotho Electronic Transactions and Electronic Commerce Bill 2013."[14]
> In July 2017, the Ministry of Communications resumed the process of reviewing and promulgating the draft bills. The first meeting of stakeholders taking place on 20 July 2017.[15]

Undermining Anonymity & Encryption Standards

In his first report to the Human Rights Council, the Special Rapporteur on Freedom of Opinion and Expression, David Kaye, notes that encryption and anonymity in digital communications deserve strong protection to safeguard individuals' right to exercise their rights:

> "Encryption and anonymity tools have become vital for journalists, activists, artists, academics and others to exercise their professions and their human rights freely, therefore laws, practices and policies that ban, restrict, or otherwise undermine encryption and anonymity — all in the name of public order or counter-terrorism — do significant, and I would say disproportionate, damage to the rights at the heart of my mandate."[16]

In the case of Lesotho, one of the main concerns for law enforcement is that of people who post anonymously on social media. To deal with this perceived threat, they have proposed to prevent anonymous activities.[17] Nevertheless,

[11] World Movement for Democracy. Democracy ALERT: Angolan Journalist Rafael Marques de Morais Accused of Criticizing the State. 23 June 2017

[12] World Movement for Democracy, ibid

[13] Too many secrets. What Washington Should Stop Hiding

[14] Resident Magistrate, Adv. Motlatsi Petrose Kolisang and Hon. Member of Parliament Adv. Lineo Irene Molise-Mabusela, Statement at the Regional Cybercrime Legislative Workshop, Port Louis, Mauritius, 20-22 August 2013

[15] According to the regulator's response to our inquiry

[16] http://www.ohchr.org/EN/NewsEvents/Pages/HRencryptionanonymityinadigitalage.aspx

[17] Interview with the Regulator on 4 June 2017

whereas law enforcement agencies are averse to social media activities that may undesirably expose their activities, the Regulator has often said 'No' to interference of free communication.

Second, the army and intelligence agencies are concerned about fake news and satire. For instance, the Regulator referred[18] to an instance when it was approached by the army about a reporter who had written a story that the King died.

> "They wanted to find out who had written that and how to deal with him despite the fact that there was a disclaimer at the bottom of the article stating that this was satirical. We had to meet with both the military and intelligence to explain to them that this was cultural. We are now living in a culture where people can say stuff- what they want to say."

The increase in the use of mobile phones to access the internet also increased challenges for law enforcement, particularly due to the dynamic allocation of IP addresses with very minimal regulator input. Law Enforcement in Lesotho, it appears, does not yet possess the expertise necessary to identify a user by linking an IP address with a specific mobile phone.

While the army and the intelligence are averse to anonymity and encryption when it comes to political and human rights issues, the Lesotho Electronic Transactions and Electronic Commerce Bill 2013 appears to uphold commercial encryption standards. Under Part II, the bill gives legal recognition and effect to electronic communications including electronic signature. Part V provides for regulation of certification authorities, and recognition of foreign certification authorities, while Part VI makes provision for compulsory registration of cryptography providers.[19]

Print and Broadcast Media Content Controls Regime

The above cases show that although Lesotho does not yet have specific laws that govern social media, it is relying on the overt track of second generation of information control in cyberspace which "aims to legalize content controls by specifying the conditions under which access [should] be denied.[20] Instruments they are relying on include the doctrine of information security as well as the application of existing laws, such as slander and defamation, to the online environment. In this case, both the army and the intelligence agencies are resorting to expanded use of defamation, slander, and "veracity" laws in an attempt to deter bloggers and independent media from airing/printing and by corollary, posting material critical of the government or specific government officials, however benignly (including satire and humor).

The Basotho Constitution and law[21] provide for freedom of speech, but the Constitution does not explicitly mention freedom of the press. The law prohibits expressions of hatred or contempt for any person on the basis of the person's race, ethnic affiliation, gender, disability, or colour. So far, the government hasn't arrested or convicted anyone under the law. Also, the law grants citizens the right to free expression, including obtaining and imparting information freely, but only as long as it does not interfere with "defense, public safety, public order, public morality, or public health."

[18] Id.

[19] See Clauses 28 and 29 respectively.

[20] Our view based on the reading of Ronald Deibert and Rafal Rohozinski Control and Subversion in Russian Cyberspace

[21] For Lesotho laws, please see: http://www.kas.de/medien-afrika/en/

The usage of libel/slander laws on the internet is an extension of their usage in respect of other forms of media and, as described below, the law has been used for reasons other than those specified therein, including for reasons political in nature.

In the case of print media, some journalists have resorted to self-censorship in order to avoid state persecution. On June 27 2016, the *Lesotho Times*' Zimbabwean publisher, Basildon Peta, was charged with unlawfully, intentionally, and seriously impairing the dignity of another, and maliciously defaming the army commander following the publication of an anonymous satirical article suggesting that civilian authorities reported to him.[22]

Such self-censorship may also be a reaction to the censorship or content restrictions placed on broadcast media. On November 10 2016, for example, non-government radio stations suddenly went off the air at the end of a live broadcast of a press conference where a faction of the prime minister's party (the DC) announced the party's withdrawal from the government's seven-party coalition. As well, in August 2016, the Minister of Communications Khotso Letsatsi reportedly called a radio station and ordered it to halt the Democratic Congress Youth League program which discussed corruption.

Also broadcast media has been shut down on two occasions:

> "On the night of 31st August 2014 when there was an alleged attempt at overthrowing the then government of Mr Thabane. The shutdown was instigated by some of his coalition partners after a fallout between them. It was not a government sanctioned move but it was an action by those involved in the coup attempt.
>
> In February 2017, a few stations (2 out of 22) were shut down for allegedly being in arrears on their rentals at the government broadcaster's transmission facilities. It is believed it was due to some new items/programmes that had aired what the government of the time did not like. But an official line from government was that they owed rentals. The transmission was restored after a court order obtained by one of the stations, PC FM."

Print and broadcast content controls not only reveal the previous government intentions with regards to the Internet (if it had acquired the knowledge and capabilities to monitor and censor Internet-based activities), but can also be viewed as an extension of a surveillance state that has previously been known for enhancing its jurisdiction over national cyberspace and expanding its powers of surveillance. As it is, the law already permits "any police officer of the rank of inspector or above [to] search individuals or homes without a warrant". If Lesotho were to have a non-vigilant or permissive regulator, these powers could easily be extended to include warrantless monitoring of internet users and usage. As a clear demonstration of its surveillance powers, "In 2014, the Intelligence Unit bought telephone tapping devices, and politicians were the first to avoid using locally registered phones and resorted to roaming as they feared to be tapped." This indicates that the policy was not well planned and did not benefit from wide support within the Government. There were also unconfirmed reports in a circular disseminated in April and May 2017 that the government acquired cyber surveillance equipment, including sting rays from a South African company.

[22] Bureau of Democracy, Human Rights and Labor, Country Reports on Human Rights Practices for 2016: https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper

Blocking, Filtering, and Throttling of Content

Blocking and Filtering

In April 2017, when we started building our community resources for censorship measurement research (i.e. test lists) for the OONI probes, an activist and lawyer we were working with reported that "People don't have a strong online presence in [Lesotho]". This stood as a potential barrier to our technical measurements.

This was confirmed in a subsequent interview with an informant from the Regulator that "Lesotho has not seen much of blocking and filtering [of websites] as most people use social media such as Facebook which is more relevant to their needs although the lack of local content remains a huge disadvantage."

Data Traffic Throttling

With regards to whether ISPs might be censoring the internet, an informant from the Regulator said, "We aren't aware of any censorship. Regulation of content falls under their respective terms of service. For instance, they censor abusive content, service is slowed down if one exceeds the allocated data, they use anti-virus software to protect clients but there are no content limitations." The Regulator was also not aware of any dual use of technologies such as Deep Packet and Content Inspection (DPI and DCI) for censorship purposes and says that should this happen, it won't be sanctioned by any known law, unless one has an order of the court.

However, civil society representatives had contrary views. The Media Institute of Southern Africa (MISA Lesotho Chapter)[23] stated that since July 2016 when the government proposed to shut down social media, Internet transmission speeds have generally been relatively slow. In particular they pointed out that "it was even very slow on the Election Day thereby disrupting and slowing down uploads of multimedia."

He could not confirm, however, whether the Government was intentionally disrupting the Internet and if so whether this was done upstream or downstream, and in the case of the latter whether there was collusion of the ISPs.

MISA's views were corroborated during our interview with a journalist who monitored elections in the Botha Buthe district. She reported having difficulties uploading her 'voting procedures compliance' report on her organisation's website.

When we asked them, the Regulator responded they were not aware the internet slowed down on Election Day or before (neither did they dispute or admit the claims).

Also, as stated above, it should be noted that the previous government consulted with both the Regulator and the internet service providers in July 2016 on its intentions to close social media.

While there is no clear evidence that government restricted or disrupted access to the internet or censored online content, according to the regulator "government has not been giving instructions for content take down because they don't know how to do it but if they knew how to, probably they could have done it."

[23] We interviewed the Director of Media Institute of Southern Africa, Lesotho, a multimedia organisation on the Election Day on 3 June 2016

Given the lack of consistency in the approaches between the government and the Regulator, it can neither be denied nor confirmed whether the government might be disrupting networks without the Regulator's knowledge. This is further complicated by the practice, observed in some neighbouring countries, whereby governments outsource such services to foreign entities; Zambia, for example, sought the assistance of a private company Huawei, in bringing down the Zambia Watchdog.[24] However, an analysis of raw data from OONI measurements did not seem to be any strong evidence of censorship happening on any other content during the testing period.[25] This does not mean that censorship is not happening at all inside of Lesotho, but only that from the specific vantage point from which we ran measurements on a set of specific URLs we could not find signs of internet censorship occurring.

It should also be noted that the Government has a limited understanding of international legal obligations in respect of the right to freedom of expression. The Government's attempt to restrict social media, for example, was not in line with international law, under which states can only have the ability to impose restrictions on freedom of expression on narrowly drafted grounds that are both legal — provided by and within laws - and necessary to protect a specific objective.[26]

The Government, for instance, did not fully explain itself in accordance with international law on why it intended to close social media. It had an opportunity to clearly explain the reasons why it intended to shutdown social media when it met Facebook representatives in the country in 2016. To back this up, the regulator stated "When they came for the meeting with government, Facebook representatives assured the government that if they knew of fake accounts, they should let them know and Facebook could take it down but government hasn't done that. They don't [take down such content or accounts] only because they don't know. We also challenged government to provide us with examples of illegal and/or defamatory content but it failed to do so".

To address the above issue, especially preventing future possible shutdowns which are not based in law, the Regulator, instead, feels that content, especially local content is crucial as it is easily understood. The regulator also suggests the creation of the office of a government social media director who would interact with people online instead of attempting to shutdown online spaces.

Cyber & Data Security Posture & Human Rights Implications

Data Protection and Privacy

The right to privacy, including from invasive data mining, is essential to a free and self-governing society and is a defining part of individual security and personal liberty. The rise of modern technologies makes it all the more important that democratic nations respect people's fundamental right to privacy.[27] In our previous paper[28], we argue that governments must protect, at once, three different forms of security: national security, commercial security and personal privacy. Personal security is a right of the people to be secure in their persons, houses, papers, and effects including in their digital lives. This form of security is a central component of the right to privacy. The protection of security is important to free societies, individual liberty, self-government, economic growth, and basic ideals of citizenship.[29]

[24] https://www.academia.edu/31116815/Internet_Censorship_in_Zambia_Policy_and_Practice

[25] Analysis by David Fifield on 10 June 2017

[26] The Universal declaration of human rights and the International covenant on civil and political rights both have an Article 19 which sets the standard and says that everyone has the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers and through any media. Also in a resolution passed in July 2016, the UN Human Rights Council described the internet as having "great potential to accelerate human progress". It also condemned "measures to intentionally prevent or disrupt access to or dissemination of information online".

[27] Arthur Gwagwa. Protecting three types of security: National security, business/commercial and Personal security on the internet. https://www.academia.edu/32796760/Protecting_three_types_of_security_National_security_business_and_Personal_security_on_the_internet

[28] Ibid

[29] For example, see the Fourth Amendment to the American Constitution.

Although Lesotho passed the Data Protection Act in 2013, it has not implemented it since it is still yet to establish the Office of the Data Protection Commissioner. The Act, inter alia, provides for the following statement of it objectives:

> "Principles for regulation of processing of personal information in order to protect and reconcile the fundamental and competing values of personal information privacy under the proposed Act and sector-specific legislation and other related matters."[30]

The Commission's functions shall, amongst others, include investigation of any complaints and alleged breaches relating to the Act and ensure compliance with the provisions of the Act.[31] At the moment, complainants can approach the court although this has not yet been tested in practice. There are also a number of data protection provisions included in the Lesotho Constitution, 1993; ICT Policy, 2005; and Communications Act, 2012, apart from those contained in the Data Protection Act, 2012.[32]

In theory, "Lesotho's privacy law makes provision for a legal infrastructure compatible with international best practices, and especially compliance with the EU Data Protection Directive, since that will be a commercial link for data flows between the EU and the Kingdom of Lesotho".[33] A good example of the protection of fundamental rights is seen in the clause relating to trans-border flow of personal information outside Lesotho. Clause 63 of the Act permits trans-border flow of personal information out of Lesotho, but only to recipients in member states implementing SADC data protection requirements. There are several requirements that must be met for the information to be transferred to recipients in the aforesaid SADC member state(s). For instance, Clause 63 (a) requires that the recipient should establish that "the data is necessary for performance of the task carried out in the public interests or pursuant to the lawful functions of [the] data controller."

The meeting of the Data Protection Law Stakeholders with the ITU on 02 April 2013 helped to raise awareness on the importance of data protection law elevating such issues as: giving effect to right to privacy, dealing with illegitimate and unlawful monitoring of individuals, and the impact of ICT technology developments on the right to the protection of personal data in commercial activities as well as in electronic government (eGov) activities. In our interview, the Regulator understood the importance of privacy in the context of national security, e.g. by affirming that "privacy is a delicate balance due to potential acts of terrorism."[34]

Similarly, when the government consulted with both the Regulator and the internet service providers in July 2016 on its intentions to close social media, according to the Regulator, "Some people posted VPNs on social media in preparation for a possible closure". This demonstrates some level of public awareness of issues around access and circumvention.

Multistakeholders' Approaches Cyber Security including Cyber Crime

In Lesotho, the Ministry of Communications leads and has overall responsibility on cybersecurity related issues. However, other cyber security stakeholders exist, including the Lesotho Communications Authority, various academic institutions, financial institutions and National Security forces. All these stakeholders have been involved in the domestication of SADC model laws at different stages.

[30] Resident Magistrate, Adv. Motlatsi Petrose Kolisang and Hon. Member of Parliament Adv. Lineo Irene Molise-Mabusela, Statement at the Regional Cybercrime Legislative Workshop, Port Louis, Mauritius, 20-22 August 2013

[31] Clause 8

[32] Presentation on Lesotho Data protection Law - ITU

[33] https://www.researchgate.net/publication/311315687_Privacy_and_Data_Protection_in_Lesotho

[34] Interview with the Regulator, 4 June 2017

The regulator stated that “There are no specific structures but as in other countries, some elements related to government adhering to international norms, and using the SADC framework where issues of governance are concerned. There is nothing codified in this area. However “whenever there is a policy or law to be introduced or changed, all stakeholders from business to academia to government itself are engaged in deliberations.”[35]

A cyber security strategy and policies were developed by the Government and submitted to Parliament for adoption earlier in 2016.[36] This was confirmed in our interview with the Regulator on 4 June 2017: “2013 draft has not yet passed through Parliament, but might pass in the next parliament/government consultative session with Parliament to understand risks, concepts, meeting again with 6 drafters and 30 stakeholders.”

While no national Computer Emergency Response Team (CERT) has been established yet in Lesotho, lawmakers discussed its creation in 2016. Mechanisms for policy and procedure related to cybersecurity will be in place once the national cybersecurity strategy has passed and implementation begins. According to the Government of Lesotho, the role of the Government will be to ensure that all citizens’ rights are observed and that the perpetrators of cybercrime will be fairly charged. Currently, “the topical issues are those relating to “abuses” of social media by some people vs government concerns regarding what it perceives as infringements on national security. Under the previous government, the extent to which they would respect the rights to privacy and freedom of expression under the ICCPR remained an open issue given the level of paranoia fuelled by unfounded national security concerns.

However as on the date of publication of this report, “the new government has not made any pronouncements or express views on issues relating to social media. However, all stakeholders and citizens recognise the need for: protection of minors, not aiding terrorism, protecting against the infringements of privacy of other and the need to prosecute criminal acts conducted by electronic means in the same way a similar incident would be treated “off-line”, e.g fraud, defamation”. There have been previous cases of cybersecurity breaches such as the usual hacks on websites and people’s accounts on social media (e.g. Facebook) from time to time by private actors. There is no specific definition or framework of cybersecurity but one might be there once the government has a cybersecurity strategy or policy but it does not have one.[37]

According to Lesotho authorities, social media is considered a substantial threat vector, as social media users are able to get away with wrongdoings due to the unavailability or unsuitability of cyber laws to investigate and prosecute cyber criminals.[38] So far, there has not been any cases relating to criminalisation of content posted on internet. However, there are cases relating to broadcast media, radio and print media that have gone to court, such as; Lekhoaba (PC FM) and the Ramahoana which is still pending over an offensive statement he made in 2014. This is in addition to governments threats and proposal to shut it down as discussed elsewhere above.

While there are no current cybersecurity awareness initiatives on-going, authorities believe that cyber awareness campaigns will only garner support and momentum once the national strategy has been passed.

It also appears that a lack of clear mandates has hampered progress towards the passage of laws and strategy formulation. The Regulator said “In 2012 the government had instructed us to come up with a cybersecurity policy; then a new Minister came up with different priorities. In 2014, we did a “Cyber Security Posture” — an inventory of where the country was as a basis to come with a good

[35] This was evident in the HIPSSA report.

[36] https://www.thehaguesecuritydelta.com/.../Cyber-security-trends-report-Africa-en.pdf

[37] Interview with Regulator on 4 June 2017

[38] https://www.thehaguesecuritydelta.com/.../Cyber-security-trends-report-Africa-en.pdf

cyber security policy/strategy but after that the government changed. The one that came said the Regulator was interfering with its mandate/space".[39]

According to a recent survey, there are currently no mechanisms in place to monitor cyber risks but Lesotho is vulnerable to cyberattacks and claims to have been victimized. Academic institutions in Lesotho are part of the team that drafted the Computer Crime and Cybercrime Bill 2013, therefore there are future plans to have specialized cyber security degrees to help train future cyber security professionals.[40] According to the same report, Lesotho is currently working hand-in-hand with other member states in order to coordinate cyber threats and the country is very committed to confidence building measures.

Coordination between countries on cyber security is being done under the International Telecommunications Union (ITU) Harmonization of the ICT Policies in Sub-Saharan Africa (HIPSA) project, in terms of which the ITU sponsored drafts of cybersecurity laws for the Southern Africa Development Community (SADC) region, and allocated its consultants to work with the respective countries. The accusation in the *Zimbabwe Daily News* and by TechZim[41] that Zimbabwe's draft Computer Crime and Cybercrime Bill plagiarised Lesotho's own Computer Crime and Cybercrime Bill does not take account of the above context, since both countries' laws are founded on the ITU draft SADC Model Law.

Good Practice in Regulation

It's also important that in 2012/2013, a representative of the Lesotho Regulator was one of the Respondents in a Comprehensive Study on Cybercrime for the UN Office on Drugs and Crime.[42] This is an indication that Lesotho has access to international best practice.

The Regulator is also a member of both the Internet Society and ITU and, according to the Regulator, "we do take note of best practice and recommendations from these bodies."

From that experience, it is evident that the Regulator was aware of some of the critical issues that ought to be considered in the application of the cybercrime law in a manner that respects human rights online.

While the Regulator has a good understanding of cybersecurity and international safeguards to protect human rights online, such knowledge is lacking in the country's intelligence and law enforcement as mentioned above.

We discussed digital forensics with the Regulator who held the opinion that "When it comes to law enforcement, there must be other forms of investigation other than the use of devices [and where devices are used, this must adhere to best practice leading to the protection of human rights]". If law enforcement followed this and other safeguards, this will ensure the respect and the security and privacy of individuals in the implementation of the pending cyber security law. We raise concerns on the use of forensic devices without proper safeguards elsewhere.[43,44]

We also asked the regulator about the need for transparency in internet regulation, they responded:

> "Transparency is a cornerstone of regulation and good governance. However, cultural norms of the members of society determine the extent of transparency exercised, for example, some information may not be held as confidential, but at the same time not shared for the simple reason that

[39] Interview with the regulator on 4 June 2017

[40] https://www.thehaguesecuritydelta.com/.../Cyber-security-trends-report-Africa-en.pdf

[41] http://www.techzim.co.zw/2016/08/zimbabweans-scream-plagiarism-discovery-proposed-cybercrime-bill-resembles-lesothos-draft/

[42] You can find the report here: https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html

[43] https://www.academia.edu/11675711/Implications_of_Zimbabwes_proposed_Cyber_Crime_Bill

[44] https://www.academia.edu/32554577/Circumvention Technologies_and_Internet_Freedom_tools_to_keep_the_Internet_Accessible

> sharing voluntarily is not a norm but is someone asked for the information they get it. You may have a look at the USF manual of operating procedures on transparency — the level of transparency is supposed to be high but not all agencies do it."

However, it is doubtful if there is a shared understanding among the law enforcement agencies, as the Regulator was of the view that "Law enforcement and prosecutors currently struggle with the use of electronic evidence which is currently not admissible or recognised under Lesotho laws. Officers lack technical capabilities, no capacity and the whole legal fraternity would benefit from relevant training."[45]

Now that Lesotho has a new government, those responsible must take the step to raise public awareness in line with the Regulator's commitment to "sensitise all the relevant stakeholders about the significance of issues relating to cybercrimes, and security of the modern, complicated and highly sophisticated cyber world in an endeavour to ensure safety and prosperity of both present and future generations therein".[46]

Intermediary Liability and Freedom of Expression

Also, on a positive note, the proposed cybersecurity laws exempt intermediaries from liability under certain circumstances. Part VI of the Computer Crime and Cyber Bill, 2013 leaves room for exoneration from liability on the part of the Access Provider, Hosting Provider, Cacheing Provider, Hyperlinks Provider and Search Engine Provider under specified conditions therein; while Part VII provides for limited liability for acts and omissions committed in good faith and without gross negligence in line with the provisions of the Act.

Part 9 of the Electronic Transactions and Electronic Commerce Bill 2013 also limits the liability of service providers provided they meet certain conditions. By describing them as 'mere conduits, the bill exempts them from liability arising when they provide hosting, cacheing and information location services. Also, there is no general obligation on a service provider to: monitor the data which it transmits or stores; or actively seek facts or circumstances indicating an unlawful activity.[47] Section 48 further protects service providers when they implement take down notices:

> "(3) Any person who lodges a notification of unlawful activity with a service provider knowing that it materially misrepresents the facts may be held liable for damages for wrongful take-down.
>
> (4) A service provider is not liable for wrongful take-down in a bona fide response to a notification of unlawful activity which complies with subsection 2."

The above provisions are very progressive in light of the increase in the censorship by proxy worldwide, whereby governments expect ISPs to monitor and censor content on their behalf. We will now briefly discuss various intermediary regimes in order to understand the Lesotho position. Under international liability systems relating to intermediaries, countries such as China and Malaysia enforce a strict liability model under which internet intermediaries are liable for content produced by others (so-called third party content). In contrast, the United States' broad immunity regime stands out as the most generous towards intermediaries. The US Communication Decency Act states, for instance, that no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by somebody else.[48]

[45] Interview with the regulator on 4 June 2017

[46] Resident Magistrate, Adv. Motlatsi Petrose Kolisang and Hon. Member of Parliament Adv. Lineo Irene Molise-Mabusela, Statement at the Regional Cybercrime Legislative Workshop, Port Louis, Mauritius, 20-22 August 2013.

[47] Section 49.

[48] Agnes Callamard, Freedom of Expression in the Globalised Age, Columbia University, 2016, although the U.S also has the safe harbour approach in the Digital Millennium Copyright Act

The “safe harbour” model occupies the middle ground:

> “In between these two extremes and the standard most common liability regime. It grants intermediaries immunity from liability provided they act quickly, expeditiously to remove or disable access to illegal information, when they obtain actual knowledge of such content. This model is at the heart of the so-called notice and take-down procedures, meaning that upon notification and a full investigation, the intermediaries must take appropriate steps which may include taking down the content that has been flagged to their attention as being illegal.”[49]

Internet Access and Connectivity & Free Flow of Information

Universal Service Fund (USF), Base Stations and Internet-based Radios

In 2016, the Internet was not widely available and almost non-existent in rural areas of Lesotho due to lack of communications infrastructure and high cost of access. According to the International Telecommunication Union, approximately 16 percent of the population had access to the Internet in 2015.[50] Lineo Tsikoane, activist and lawyer we collaborated with confirmed that “People don’t have a strong online presence in [Lesotho]”.

The Universal Service Fund (USF)

However, the Universal Service Fund (USF) has been helping the country to increase mobile base stations in remote areas. The Communications Act 2012 and prior to that the LCA Act 2000 addressed the need for and means to achieve universal access to communication services.

The USF is mainly focussing on mobile access to voice and broadband services in the rural areas since private service providers are paying more attention to the more commercially viable areas. The USF is being used as the main mechanism for addressing rural connectivity and digital literacy challenges. To date 96% of inhabited areas have access to either a 3G or 4G network. The target is to close the gap by 2020. The study commissioned last year by the USF has shown that in some or the highlands areas, 90% of the people had not used or did not know what the internet was. This represents over 60% of the population. The problem can be phrased as follows: There is coverage but people lack awareness of the service and its benefits. Now the government is pushing for the provision of government services online as a way to improve access and convenience for citizens. This expected to be a stimulant for adoption by people that had not found internet relevant in their lives hitherto.

Data costs

Data costs are generally low or on par with some when compare to other SADC countries. To illustrate this, 1 LSM (M) = 1 ZAR. Following is an example of the pricing of bundles from Econet Telecom Lesotho whose prices are comparable to some extend with other providers of similar services:

[49] Agnes Callamard, Freedom of Expression in the Globalised Age, Columbia University, 2016

[50] U.S. DOS Bureau of Democracy, Human Rights and Labor, Country Reports on Human Rights Practices for 2016, https://www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm#wrapper

a) Wi-Fi voucher: M3.00 for 15 minutes; M5.00 for 30 minutes; M8.00 for 60 minutes (some sell Wi-Fi voucher for data bundles in MB though).

b) Social media bundles (Facebook & WhatsApp combine – there are separate offerings respectively for either Facebook or WhatsApp for lower charges): Daily: M5; Weekly: M20; Monthly: M60

According to the regulator: "price movement are a factor of market dynamics, and not so much regulation. Prices are not regulated that much, rather business practices to aimed at the protection of consumers e.g, in areas of the terms and conditions of service, their fairness, and enforcement of approved terms."

The Undersea Cable and Internet Exchange Point (IXP), and Infrastructure Sharing

Lesotho could also substantially boost access and connectivity if it fully utilises its infrastructure.

Gateways

Each telecommunication company has its own gateway, as the country did away with a single gateway policy," Every licensed network operator has the right to interconnect internationally for both voice and data. There is no such thing as "gateway" in the regulatory or legal vocabulary. It was removed in 2007."

Unlike in Zimbabwe, where proposals for a single gateway have been criticised for the likelihood in the increase of state surveillance, multiple gateways in Lesotho lessens the government's upstream surveillance capabilities. They must do so via proxy in terms of which they require the private companies to create backdoors for it.

IXP

The country also has an Internet Exchange Point (IXP). The regulator assisted in the establishment of the IXP and continues to do so. The regulator is supportive of the IXP association which is the industry's own association for this purpose. Government is also supportive and wanted to peer but ended up not be able to due to other challenges in its own network.

Data centre

The government has its own data centres, and the private sector players are free to establish their own. There is no specific regulation in this space and it is a market that is expected to grow with wider adoption of business and government going digital.

Undersea cable and Infrastructure sharing

Lesotho has its own undersea cable currently not being fully utilised due to disjointed policy and a lack of political commitment. The lack of political commitment may be due to quick successive governments with different policy priorities.

There is also an infrastructure sharing agreement in place in terms of which a telecommunications company applies to another telco to agree on sharing terms and conditions. If they fail to agree terms, they approach the Regulator.

Impact of USF on Freedom of Expression

As a result, the USF has also in turn facilitated free flow of information. According to the Regulator who showed us a map of new and proposed base stations, "The USF has changed the political landscape. Before, people didn't have access to information. For example, now in constituency 77 they have PC FM Radio which one can tune in through an internet –based application to listen to political programmes". For example, the Lesotho Soul Radio App[51] allows a user to access links to all available radio stations via the app user interface.

There was a sentiment that the increase in the free flow of information opened up space which enabled people to make informed choices during the elections. "This also coincided with Lesotho's 'Facebook Era' which increased in real popularity after the 2015 elections. Whereas, the elections in 2015 and prior, did not benefit much from Facebook, one can see a change in political discussions during the 2017 elections", said the Regulator.

Those interviewed also felt that WhatsApp[52] is facilitating the rising awareness; for example, those with access to online radios also record broadcasts with political content and send them via WhatsApp to their families in the countryside. The opposition leader, Thomas Thabane, predominantly won in constituents with a dynamic media while the incumbent held in areas with a predominantly government media.

The MISA Director, Tsebo Mats'asa also confirms the above by writing:[53]

> In Lesotho, Facebook has turned out to be a vibrant platform for political participation. Individual members of the public post their political views while on the other hand fanatics of political parties create groups that discuss political issues ranging from, events, official and unofficial decisions to statements by the government and leaders of political parties. There are no daily newspapers in Lesotho and broadcasting sector is unethically run. As a result Facebook has become a daily source of information whose content, most of the time, is received with mixed feelings and varying interpretations among ordinary citizens, political fanatics and their leaders. Lesotho is a country where official information is so limited that citizens depend on roamers and gossip. This makes social media, especially Facebook that this article is about, to be one of the platforms where information is shared daily. While Facebook role as information sharing platform may be acknowledged as a positive, a challenge with information on Facebook is poor credibility and meagre authenticity as active sources on the platform are either anonymous or use pseudo names. Despite this challenge, it is however, undisputable that political information posted on Facebook in Lesotho, most of the time turns out to be true and it puts a lot pressure on both the government and political leaders.

[51] www.soul.co.ls

[52] An internet based social application for communication.

[53] Newsline 365 Facebook in political participation: https://newsline365.wordpress.com/2016/01/05/facebook-and-political-participation-in-lesotho/, 5 January 2016

Remaining Key Challenges

Despite these agreements, barriers to access and connectivity still remain which should not be the case in a country of about 2, 5 million people. Some of the barriers identified during our interviews include:

- **A lack of awareness**
  There is low level internet literacy as most people only know Facebook, WhatsApp, and Instagram.
- **Media-specific level barriers**
  There are few bloggers, bloggers cannot sustain their blogs as there are no adverts, and there is a need to sensitise and market blogs, especially civil society organisations
- **A lack of local content**
  Local content can amplify the presence of civil society organisations, especially those working on LGBT issues. They have Facebook pages and websites but generating content is a challenge (although MISA tries to help).

Government websites are dormant, as it seems that people do not know what use to make of them. Future capacity building should be directed at the Government, and help people access government information, as this is hindering an open government.

For more information, visit **https://www.cipit.org**, or contact **Arthur Gwagwa** at **arthurgwagwa@gmail.com**.

WHEN GOVERNMENTS DEFRIEND SOCIAL MEDIA

A study of Internet-based information controls in the Kingdom of Lesotho with a particular focus on the period around the 3 June 2017 General Elections

Arthur Gwagwa
Senior Research Fellow

Centre for Intellectual Property and Information
Technology Law, Strathmore Law School
Strathmore University, Nairobi, Kenya

Design by Anqi Li, Access Now