State of Internet Freedom
in **Botswana** 2019

Mapping Trends in Government Internet Controls, 1999-2019

CIPESA

Table of Contents

Credits _____

This research was carried out by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) with support of various partners.

This research documents the trends in government internet controls, 1999-2019 in Bostwana tracking key trends in recent years, analysing the key risk factors, and mapping notable developments on data protection and privacy legislation and violations, and users' understanding of protecting their privacy online. Other country reports for Burundi, Cameroon, Chad, the DRC, Ethiopia, Kenya, Malawi, Nigeria, Rwanda, Senegal, Tanzania, Uganda, and Zimbabwe. The research was conducted as part of CIPESA's OpenNet Africa initiative (www.opennetafrica.org), which monitors and promotes internet freedom in Africa.

CIPESA recognises Dr. Batlhalefi Tutwane as the main content contributor to this report.

Editors
Ashnah Kalemera, Victor Kapiyo, Paul Kimumwe, Lillian Nalwoga, Juliet Nanfuka, Edrine Wanyama, Wairagala Wakabi, PhD

1

Introduction

1.1 Introduction

The southern African nation of Botswana is often highly ranked on indices that measure the level of democracy and press freedom. It is also ranked as one of the least corrupt on the continent and has the fourth highest per capita income.[1] However, recent years have seen a slide in the country's democratic credentials and internet freedom is no exception. The country has adopted some measures, including retrogressive policies and laws, which curtail internet freedoms.

Various provisions of the Botswana Penal Code criminalis free speech, including defamation (sections 192-199); section 93 of the Penal Code restricts abusive, obscene or insulting language in a public gathering directed towards the President, Members of Parliament and any public officer. Section 95 of the Code outlaws threatening breach of the peace or violence.

Although Botswana has an ICT Policy and a National Broadband Strategy to drive nationwide ICT penetration, technology adoption in the country remains low as the government is yet to implement its ambitious policies for the universal roll out of ICT and digital literacy programmes. Additionally, the slow speed of the internet and high data costs have remained an impediment to access and affordability for many citizens.

Nonetheless, over the years, the government has embraced digitalisation, e-government and digital identity programmes that require citizens to provide detailed personal information.

While these measures have been embraced by sections of the population as necessary to enhance the delivery of government services and government's capacity to fight terrorism, ensure public order and cybercrime, state actors have abused the enhanced capacity to conduct surveillance and interception of private communication, and intern compromised citizens' digital rights such as privacy, expression and access to information. Besides, the implementation of these measures in the absence of key safeguards is a threat to the very rights sought to be protected. It is therefore important to contextualise the on-going discussions around digital rights by analysing the trends in how government policies and practices have shaped and restricted these rights in Botswana over the last 20 years.

---

[1] *World Bank, GDP per capita (current US$) - Sub-Saharan Africa, https://tinyurl.com/uvo6oay*

1.2 Aim and objectives of the Study

This research documents how government controls of the digital space between 1999 and 2019 have shaped and influenced internet freedom in Botswana. Specifically, the study traces the trends and developments in the digital space during this period while also focussing on the proliferation of retrogressive or repressive policies and laws; surveillance and surveillance capacity of governments; digitisation programmes; censorship; and new frontiers like the introduction of internet related taxes.

The study also identifies and recommends measures that different stakeholders – governments, civil society, technology companies, academia, media, and researchers - can take to secure internet freedom in Botswana.

2 Methodology

The study employed a qualitative approach including literature review, policy and legal analysis, and key informant interviews with purposively selected respondents. Past studies, media reports, academic works, government documents, and other literature, were also reviewed. The literature review generated an understanding of the developments in Botswana.

The legal and policy analysis included a review of relevant laws, policies and practices in Botswana. Such laws and policies include those that govern the telecoms sector, the media, social media use, access to information, interception of communications, security and intelligence agencies, and security enforcement in general.

Key informant interviews were conducted with purposively selected respondents who included staff of private companies, telecom firms, Internet Service Providers, ministry of ICT, journalists, social media users, human rights defenders and activists, academics and lawyers.

3

Country Context

3.1 ICT Status

Botswana has a small population of 2.3 million people[2] accompanied with impressive statistics on mobile money uptake and mobile phone subscriptions. As of March 2019, the number of mobile phone subscribers was 3,353,337, representing a penetration rate of 164%. Meanwhile, there were 40,000 fixed broadband subscriptions in the country, implying that most people who went online did so using mobile connections.[3]

Botswana is one of the countries with the largest Gross Domestic Product (GDP) per capita in Africa (about USD 8,263 in 2019) There has been considerable investment in laying of fibre optic cables across the country by private actors and the government. Moreover, Botswana has clear policies to guide ICT development and use, including by government departments.

The Botswana government is yet embraced e-governance, as most government services and transactions are still paper-based. Citizens still need to stand in long queues to do basic transactions. However, a few private institutions, such as banks and mobile phone companies, have introduced applications that enable their customers to do transactions either on their phones or on the internet.

For instance, the largest mobile phone service provider, Mascom, has MyZaka (slang for "my money") application that allows customers to receive and send money and to pay utility bills.[4] Orange Botswana has Orange Money, which in 2018 accounted for 73% of the mobile money market.[5] Botswana Telecommunications Corporation (BTC) has Smega (also slang for "money") which also allows one to send and money and pay utility bills.[6] In Botswana, mobile money has grown into a large industry with 1,149,673 subscribers as of March 2019, up from 412,126 in March 2015.[7]

---

[2] *Worldometers, Botswana Population, https://www.worldometers.info/world-population/botswana-population/*

[3] *Botswana Communication Regulatory Authority statistics, https://www.bocra.org.bw/telecoms-statistics*

[4] *Mascom, MyZaka, https://www.mascom.bw/about-mascom-myzaka/*

[5] *Botswana Guardian, Orange rules the Money Market, https://tinyurl.com/tj56lug*

[6] *BTC launches revamped mobile money wallet, https://tinyurl.com/wkhc3ax*

[7] *Data from Botswana Communications Regulatory Authority (BOCRA) https://www.bocra.org.bw/telecom-statistics1*

Major concerns about internet access and usage in Botswana include digital literacy and digital security. Ironically, both were identified in the ICT Policy (2007) and the Broadband Strategy (2018) as critical issues to be addressed.[8] For instance, Section 5 of the ICT Policy seeks to address the issue of security of information systems and networks. A "culture of security" was to be built through legislation and policy.[9] Indeed, a Cybercrime Crime and Computer Related Crimes Act was introduced in 2007 and amended in 2018 but the government has identified loopholes that need to be remedied.[10] A Data Protection Act was also enacted in 2018 to protect citizens and consumers data in digital space.[11]

3.2 Political Environment

Botswana is one of a few countries on the continent that are classified as having flawed democracies - as most countries are characterised as authoritarian or semi-authoritarian.[12] The country has not experienced any major political incidents and has for years been among the most peaceful in Africa. The Botswana Democratic Party (BDP) has dominated political leadership since the first democratic elections in 1966. Ketumile Masire served as Botswana's second president, taking over from the late Sir Seretse Khama in July 1980. He voluntarily retired from office in 1998 and was succeeded by Festus Mogae who finished his second term in 2008 handing over power to Ian Khama,[13] whose tenure expired in 2018 and he was succeeded by Dr. Mokgweetsi Masisi.

However, the situation became volatile in April 2018, when the former president Khama engaged in a tussle with his successor Dr. Masisi. The source of conflict seems to be Dr. Masisi's reneging on a secret deal to make the younger brother to his predecessor a Vice President of the country. One major newspaper has been reporting consistently about a plot to overthrow the current president.[14] Ultimately, the country's intelligence unit, the Directorate on Intelligence Services admitted in July 2019 that indeed the president's life was under threat.[15]

8 Botswana Broadband Strategy, https://tinyurl.com/ufajobh
9 Maitlamo ICT Policy 2007 (p. 35).
10 NBS, 2018
11 Botswana Data Protection Act, 2018, https://www.bocra.org.bw/sites/default/files/documents/DataProtectionAct.pdf
12 Democracy Index 2018 https://www.eiu.com/topic/democracy-index; Africa is home to only one fully fledged democracy https://qz.com/africa/894326/nigeria-south-africa-kenya-and-tanzania-fail-to-improve-on-global-corruption-index/
13 http://www.botswanaembassy.org/page/history-of-botswana
14 Sunday Standard (2019), 'Masisi foils Israeli sponsored coup', Sunday Standard Online, Jan. 21 : http://www.sundaystandard.info/masisi-foils-israeli-sponsored-coup, Sunday Standard (2019), 'BDF on red alert in anticipation of coup', Sunday Standard online, March 25: http://www.sundaystandard.info/bdf-red-alert-anticipation-coup [Accessed September 4 2019].
15 The Patriot on Sunday (2019), 'Masisi's life in danger', The Patriot online, July 11: https://www.thepatriot.co.bw/news/item/7238-masisi%E2%80%99s-life-in-danger.html [Accessed September 4 2019].

3.3 Economic Status

On the economic front, Botswana has for decades been a success, having one of the fastest economic growth rates in the world in the 1990s. As of 2018, Botswana was reported to have had the third highest (after Angola and Benin) Gross Domestic Product (GDP) per capita in Sub-Saharan Africa at USD 8,258, according to the World Bank.[16] The country generally has a good economy, with inflation often kept under 6% by the Bank of Botswana. In July 2019, the rate was 2.9%.[17]

Being landlocked, Botswana relies heavily on its neighbour South Africa for goods and services. However, significant diamond wealth, good governance, prudent economic management and a relatively small population, have enabled Botswana to become an upper middle-income country.[18] Between 1991 to 2017, unemployment remained a big challenge with an average rate of about 20%. Moreover, for many employed persons, salaries are very low, and the country has wide income disparities.[19] In rural areas, majority of the population depends on subsistence agriculture, with poor rains in the semi-arid climate often affecting yields.

16   World Bank, GDP per capita (current US$) - Sub-Saharan Africa, https://tinyurl.com/uvo6oay
17   Data from Bank of Botswana: http://www.bankofbotswana.bw/assets/uploaded/MPR%20_August%202019_1.pdf. Accessed 6 September 2019.
18   World Bank, Botswana Overview, https://www.worldbank.org/en/country/botswana/overview
19   See http://www.sundaystandard.info/botswana-third-most-unequal-country-world

4
Results

This section traces the history, evolution and shifts of internet control measures in Botswana since 1999. It also examines the political and socio-economic considerations behind these control measures.

4.1 Key Trends of the Internet Control Over the Last Two Decades

4.1.1 Weaponising the Law to Legitimise Actions

Like many other African countries, Botswana has introduced provisions in its ICT-related laws and policies that infringe on digital rights. As ICT usage grew since the year 2000, the provisions have become more restrictive – providing for state surveillance, interception of private communication, and online censorship, among others.

Legalising Surveillance, Censorship and Interception of Communication

In Botswana, like in many other countries in the world, there is a general concern that national laws regulating the state's surveillance of private communications are inadequate or non-existent, resulting in unlawful and arbitrary interference with individuals' right to privacy.[20] Surveillance and interception of private communication is provided for under the 2007 Intelligence and Security Service Act (ISSA). Section 22 of the Act provides that in the event that the Directorate of Intelligence and Security Services (DISS) wishes to conduct an investigation of a personal or intrusive nature such as searches or interception of postal mail, electronic mail, computer or telephonic communications, the Director General or an officer or support staff authorised by him or her shall show cause to a court of Senior Magistrate or above or a Judge of the High Court and obtain an order in a secret hearing.

However, an examination of the interception regime for private communications under the ISSA clearly demonstrates that the law fails the principle of proportionality as it does not provide adequate supervisory and monitoring mechanisms over interception of private communications and therefore fail to ensure that an interception would be the least intrusive and proportionate to the interest protected.[21]

---

[20] *Badala Tachilisa Balule et al (2015) Balancing the Right to Privacy and the Public Interest: Surveillance by the State of Private Communications for Law Enforcement in Botswana; Statute Law Review, 2015, Vol. 00, No. 00, 1–14*

[21] *Ibid*

Silencing Dissent and Criticism through Criminalising Free Speech

The use of criminal law to prosecute and punish critics has been reported in Botswana. For example, Section 93 of the Penal Code restricts abusive, obscene or insulting language in a public gathering directed towards the President, Members of Parliament (MPs) and any public officer. Further, section 95 outlaws threatening a breach of the peace or violence; section 96 prohibits incitement to violence and disobedience of the law; section 140 prohibits writing or uttering words with intent to wound religious feelings. While the offences do not specifically mention the online context, the provisions can still be used to charge persons who commit the offences online. In September 2016, there were reports of the arrest of a 36-year-old computer technician by the Botswana security services who was alleged to have created the controversial photoshopped image of a nude President Lieutenant-General Seretse Khama.[22]

In 2015, a tabloid journalist Daniel Kenosi, was arrested and charged with defamation and the unlawful distribution of obscene material contrary to section 16 of the 2018 Cybercrime and Related Crimes Act, in connection with social media posts implicating a government minister in a sex scandal that the journalist had published in early 2015.[23]

In May 2016, the offices of the Botswana Gazette were raided and three staff temporarily detained over a news report implicating the DISS and Botswana Democratic Party in corruption. One of the journalists was charged for disclosing information related to an ongoing investigation. In addition, Outsa Mokone, an editor of Sunday Standard, was charged with sedition but later acquitted, following a story published in the newspaper alleging that the president was involved in a late-night car crash that was not reported to the police.[24]

4.1.2 Disrupting Networks – From Cyber-Attacks to Media Blockage

The use of cyber-attacks has been noted in Botswana. In January 2016, Mmegi, an independent newspaper in Botswana, experienced a cyber-attack that destroyed a significant amount of its archived material.[25] Mmegi's editor claimed that the Directorate of Intelligence and Security Services (DISS) was behind the attack, and that it had been carried out as retaliation for an article claiming that the Directorate on Corruption and Economic Crime (DCEC) had questioned the former head of DISS about the wealth he had purportedly amassed.

According to the Sunday Standard newspaper, in 2014, one radio station deemed critical of the government, Gabz FM, reported that their signal was jammed and were briefly off air. According to media reports, other private radio stations, including Duma FM and Yarona FM experienced similar problems.[26]

---

22 *The 36-year-old suspect a computer technician, has been flown to Gaborone, where he remains in detention*
    https://citizen.co.za/news/news-africa/1289433/botswana-police-arrest-suspect-of-nude-president-khama-image/
23 *Freedom House (2017) Freedom of the Press 2016/Botswana https://freedomhouse.org/report/freedom-press/2016/botswana*
24 *Outrage over sedition charge against Botswana journalist, https://tinyurl.com/yx7poh4g*
25   *Freedom House. (2016). Botswana : Freedom in the world. https://freedomhouse.org/report/freedom-world/2016/botswana*
26 *Sunday Standard (2014) DISS/MI launch electronic warfare attacks against private media*
    https://www.sundaystandard.info/diss-mi-launch-electronic-warfare-attacks-against-private-media/

4.1.3 Surveillance Galore: The Build-Up of States' Capacity

The country's security intelligence services, especially the DISS, have been used as ideological state apparatuses, rather than for public good.[27] They served the interests of the president and his ruling colleagues. During this period, DISS and the Military Intelligence Unit are suspected to have acquired state of the art surveillance equipment from Israel in the run up to the 2014 general election, with capability to spy on both the internet and telephone conversations and jam radio and mobile signals. The country's military intelligence unit is also believed to run a separate surveillance operation. Right at the outset when the 2008 Intelligence and Security Services Act was rushed through Parliament on the eve of his presidency, president Khama appointed a close friend from his army days, retired Colonel Kgosi, as the head of this intelligence agency. This ensured that this agency was under his grip and would be loyal to him rather than the laws of Botswana.

In 2014, Khama was blamed for transforming Botswana "into a surveillance state", leading to "fear and paranoia" and the loss of "the very peace of mind he claimed to be protecting."[28] The Parliamentary Committee of the Intelligence and Security (PCIS) was criticised for being weak in its oversight role, as its members are appointed by the President. Hence, it lacked independence from the executive, and access to critical information relating to DISS thus was rendered clueless on DISS operations. In February 2014, it was revealed that DISS had acquired reconnaissance equipment from a German-based company to spy on opposition politicians, journalists and human rights lawyers.[29] The surveillance technology called FinSpy Mobile and FinSpy PC is capable of infecting computers and mobile phones on a mass scale with malware and allows remote monitoring of user activity and siphoning of data from the devices.[30]

It is apparent that this organisation operated outside the legal framework because in 2010 another former army commander, retired Major General Pius Mokgware, who was then a member of the opposition, had discovered that his private mobile phone had been spied on by the Botswana Defence Force (BDF) intelligence services working with the DISS and the government-owned mobile services company, BTC. He received a SMS from a BDF agent, Dzikamani Mothobi, who had sent it to him by mistake. The message revealed to him that he was being spied on. In his investigations, he discovered that a BTC employee, Modise Mokgatlhong, working for the subsidiary Bemobile had provided his mobile details to Mothobi. Subsequently he brought a 6 million-pula (USD$ 600,000) lawsuit against the army, BTC and the Attorney-General of Botswana at the High Court. Mokgware established that he was under surveillance for at least three months, between December 2009 and February 2010. The matter was settled out of court in 2013 to save the face of the intelligence services in what was believed to be a very expensive settlement running into millions of pula.[31]

It was also reported that Military Intelligence agents had completed training on the new equipment and ran test runs jamming all three private radio stations: Duma FM, Gabz FMand Yarona FM for about 10minutes. There were fears that the equipment could be used against the media during the 2014 elections.[32]

27 Branston, G. and Stafford, R. (1996), The Media Student's Book. London and New York: Routledge
28 Khama turns Botswana into a surveillance state, https://www.sundaystandard.info/khama-turns-botswana-into-a-surveillance-state/
29 Botswana Guardian (2015), 'DIS launches massive surveillance operation', Feb. 23:
    http://www.botswanaguardian.co.bw/news/item/1284-dis-launches-massive-surveillance-programme.html
30 DIS launches massive surveillance operation, https://tinyurl.com/w4j6qlz
31 Mmegi (2013), Mokgware's espionage case moves out of court, http://www.mmegi.bw/index.php?sid=1&aid=1167&dir=2013/february/Tuesday19
32 Khama/Kgosi Network of Shady intelligence security gig shots has DISS big shots over the barrel,
    http://www.sundaystandard.info/khamakgosi-network-shady-intelligence-security-big-shots-has-diss-over-barrel (Accessed 9 Sept. 2019).

4.1.4 The Push Towards Determining Identity Amidst Poor Oversight

SIM Card Registration

In 2008, the Botswana Telecommunications Authority (BTA) announced a 17-month registration exercise for all prepaid mobile phone SIM cards, to run between September 2008 and December 2009. During the announcement, the BTA Chief Executive, Thari Pheko, is reported to have said that the registration would help in the fight against crime by availing information on each SIM card as well as allow the tracking of people who use cell phones to commit crimes.[33]

Although there is a perception that SIM card registration is useful to prevent cybercrimes, little attention is paid to the potential misuse of personal data that is collected during the registration process for unauthorised surveillance of key groups such as whistle-blowers, human rights defenders, the political opposition and the media.

Adoption of Biometric Data Collection

In 2010, Botswana completed the installation of the Automated Fingerprint Identification System (AFIS) at police stations across the country. It was notably alleged that the system would reduce p waiting time from a week to two days for persons seeking police clearance, such as r students going for training abroad, passenger service vehicle licence applicants. With the AFIS, fingerprint technicians would be able to scan fingerprint images into a database for easy storage, retrieval, and comparison.[34]

On the other hand, the Botswana National Registration Act Cap 01:02, makes it mandatory for every citizen of Botswana to undertake National Registration within 30 days of attaining the age of 16 or within 30 days of acquiring Botswana citizenship. During the registration process, the following information is obtained: name; date of birth; sex; residential and postal address; place of birth; marital status; occupation; and information on parents or other family members. Additionally, fingerprints (two thumbs) are captured as part of the personal identification data.[35]

The National Identity Management System is linked with other systems, such as the electoral system, the Social Benefit Registration System (SOBERS), government payroll, and the transport system.[36]

---

[33] Date set for SIM-card registration http://www.mmegi.bw/index.php?sid=1&aid=9&dir=2008/July/Thursday10/

[34] http://www.gov.bw/en/Ministries--Authorities/Ministries/State-President/Botswana-Police-Service-/news1/Automated-Fingerprint-Identification-System/

[35] ID4D Country Diagnostic: Botswana http://documents.worldbank.org/curated/en/864651486101539760/pdf/Botswana-ID4D-DiagnosticWeb040418.pdf

[36] https://citizenshiprightsafrica.org/id%C2%ADentification-syst%C2%ADems-analysis-country-assessment-botswana/

4.2 Key Positive Trends

Despite the negative trends that hindered internet freedom and digital rights in past years, there were also some positive developments to advance online freedom of expression in Botswana. They included the adoption of progressive legislation and advocacy by non-state actors.

4.2.1 Adoption of Progressive Legislation

Beginning 2007, the government has enacted several laws to promote digital security and online responsibility. Some of these measures were meant to criminalise computer abuse such as computer crimes, fraud and other banking related crimes.

The Cybercrimes and Computer Related Crimes Act, 2007 (amended 2008)[37] is generally regarded as a progressive law that follows the regional and global trend to deal with crimes committed in digital space or using computers. For instance, it deals with crimes like access to a computer system with intention to commit a crime or facilitate commission of a crime and crimes like cyber-stalking and revenge pornography.

Section 17 of the Act prohibits the unlawful disclosure by service providers of information collected, and provides a maximum penalty of 40,000 pula (USD 3,882), or to imprisonment for a term not exceeding two years, or to both.

More recently, the Data Protection Act (2018) was enacted to protect the data and privacy of Botswana citizens These measures were informed by legislative movements in other parts of the world. A good example is the General Data Protection Regulation of the European Union which came into force in May 2018. This law seeks to protect the privacy of individual citizens in the EU and EU economic area and governs the transfer of their personal data outside the EU and the EU economic area.[38]

Similarly, the Electronic Records Evidence Act (2014)[39] is a progressive law meant to facilitate admission of electronic evidence in court. This was developed to enable the country keep abreast with developments in technology globally. This law was an amendment to the Penal code which until then, did not recognise electronic records. It empowered the regulator, BOCRA, to help with the preparation of such evidence. Before 2014, the admissibility of electronic evidence in court was at the court's discretion.

---

37 Text of the law https://www.bocra.org.bw/sites/default/files/documents/18%20Act%2029-06-2018%20Cybercrime%20and%20Computer%20Related%20Crimes.pdf

38 See for instance: CIPESA, "Challenges and Prospects of the General Data Protection Regulation (GDPR) in Africa," https://cipesa.org/?wpfb_dl=272

39 Text of the law https://www.bocra.org.bw/sites/default/files/Electronic%20Records%20and%20Evidence%20Act%202014.pdf

4.2.2 Advocacy and Push-back by Non-State Actors

The rule of law is entrenched in Botswana and the independence of the Judiciary is highly valued. However, during the presidency of Ian Khama, the government sometimes ignored court orders but eventually was prevailed upon to respect them. A prominent example is the refusal to appoint attorney Omphemetse Motumise to the bench in 2015 but the threat of further legal action forced the hand of government in 2017.[40]

Additionally, surveillance by the DISS newspapers wrote many stories exposing maladministration in the surveillance practices of the DISS. In 2017, the Directorate on Corruption and Economic Crime (DCEC) went to court in a bid to stop the Sunday Standard newspaper from reporting on criminal investigations relating to the then DISS Director Isaac Kgosi. However, the High Court allowed publication of stories on the matter to continue provided they did not disclose the names of certain parties to the case.

[40] *Mmegi (2017), 'Khama finally appoints Motumise to the bench', Aug. 17: http://www.mmegi.bw/index.php?aid=72455&dir=2017/october/17*

5
Conclusion and Recommendations

5.1 Conclusions

The study has found that successive governments since 1999 have broadened the range of measures that control the use of digital communications including the internet. The implementation of oppressive provisions in laws is on the rise and it is evident that the state has attempted to use legislation to legitimise practices which are otherwise unlawful to impose restrictions and internet controls.

While laws in place are touted as necessary towards fighting cybercrime or enhancing cybersecurity in the country, they have often been directed towards clamping down on criticism and quelling dissent.

A few of the laws enacted during the period under review promote internet freedom rather than curtailing it. Unfortunately, the biggest weakness has been poor public administration and implementation, driven by the questionable behaviour of the DISS that caused fear among citizens connected to digital technologies.

5.2 Recommendations

Government:

- Mobilise citizens on the digital literacy programmes that are comprehensively discussed in both the ICT Policy (2007) and Broadband Policy (2010, 2018) to enable their acceptance and usage.
- Protect and respect human rights and freedoms as enshrined in the constitution and in international instruments that Botswana has ratified.
- Stop the use of regressive internet control policies and practices and instead promote the use of the internet through adoption of favourable laws and policies.
- Ensure that sufficient safeguards and principles including 'privacy by design' are included in laws and policies for the robust protection of the right to privacy and personal data.

Media

- Media managers and editors should promote digital safety and the protection of journalists through adoption of policies that progressively promote online safety and security.
- Report, cover and highlight incidents relating to threats to internet freedom so as to garner mass awareness and support for internet freedoms.
- Media managers and editors should actively build their capacity and knowledge on internet freedom issues.

Civil Society

- Collaborate to promote internet freedom through active monitoring, advocacy, research and public interest litigation for a favourable environment that facilitates the understanding and enjoyment of internet freedoms

Academia

- Conduct evidence-based research on digital rights
- Include internet freedom in curriculum development to build awareness on the various digital rights and related issues
  .

Technical Community

- Educate stakeholders on the impact of new technologies on internet freedom.
- Develop and promote local platforms which promote public engagement and internet freedom.
- Develop and promote innovative technologies to circumvent internet control restrictions and surveillance.
- Create awareness on digital safety through training for the public e.g. on the use of virtual private networks (VPNs), encryption, anonymous browsing, malware and spam.

CIPESA