State of Internet Freedom in Africa 2018

Privacy and Personal Data Protection in:

Challenges and Trends in Zimbabwe

September 2018

CIPESA

Table of Contents

State of Internet Freedom in Africa 2018
Privacy and Personal Data Protection: Challenges and Trends in Zimbabwe

1 Introduction and Background

The concepts of privacy and data protection go hand in hand.[1] In Zimbabwe, societal ideas around privacy are complex and are mostly framed in the 'nothing to hide' lens and a general lack of full understanding of their meaning. Zimbabwe does not have a data protection law and because of this, the government and private companies continue to collect and process personal data without clear legislative and regulatory mechanisms.

Moreover, the country has several legal provisions that allow the government to conduct surveillance without sufficient oversight and users of Information and Communications Technology (ICT) continue to face regular harassment for their online activities.[2] There are reported cases of users' personal data being used for unlawful purposes, including being processed without the permission of the data subject, which conflicts with the constitutionally guaranteed right to privacy.

In the period leading to the 2018 elections, there were allegations that personal data held by the electoral and telecommunications commissions may have been abused for political gain of the ruling party.[3] At the peak of the election, the ruling party, ZANU PF, bombarded[4] thousands of registered voters with campaign messages via SMS, raising concerns over the security of people's data held by public bodies and the Zimbabwe Electoral Commission (ZEC) in particular. The ZEC is one of the public bodies in charge of one of the biggest databases containing people's personal data. The electoral body was accused of giving away private citizens' information to ZANU PF, but it was quick to deny this and shift blame to mobile companies.

1 *See: https://theoutline.com/post/4409/stop-saying-privacy-start-saying-data-protection?zd=1&zi=h4eo3dmi*

2 *Freedom of the Net Zimbabwe 2017. https://freedomhouse.org/report/freedom-net/2017/zimbabwe*

3 *See: https://bulawayo24.com/index-id-opinion-sc-columnist-byo-140062.html*

4 *https://www.newsday.co.zw/2018/07/nuisance-campaign-messages*

In October 2017, the government set up a short-lived[5] Ministry of Cyber Security, Threat Detection and Mitigation supposedly to deal with fake news, "abuse" of social media and infractions committed over these networks. Its creation portended bad times for many Zimbabweans, especially those that depend on the anonymity and freedom afforded by the internet to criticise those in power. The internet is still the one frontier where Zimbabweans feel freer and safer to criticise the ruling party and government officials. Though the ministry ceased to exist, the Computer Crime and Cybercrime Bill,[6] which it was to preside over, is still in development and there is no clarity in terms of when it might be passed. This Bill is a source of great concern among civil society because of its draconian provisions, and there were further concerns that its passing into an Act would be hastened ahead of the election, however this did not happen.

The government is also alleged to have entered a facial recognition project partnership with a Chinese company – CloudWalk Technology.[7] The terms of the partnership are that the Zimbabwean government will give away massive databases of its citizens. Earlier in 2018, it emerged that the Chinese had spied on the African Union for over five years.[8] That the Zimbabwe government then went on to volunteer its citizens' personal data for facial recognition experiments with China raises a lot of ethical, legal and security concerns.

This research therefore sought to document the state of privacy and personal data protection in Zimbabwe. It tracks key trends in the country over the past five years, analysing major risk factors, mapping notable developments on data protection and privacy legislation and violations, and identifying measures that can positively influence the right to privacy legislation in Zimbabwe.

---

5 *The Ministry stopped existing after the coup of November 2017.*

6 *https://www.techzim.co.zw/2016/08/heres-zimbabwes-draft-computer-crime-cybercrime-bill - Accessed 27 June 2018.*

7 *https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity*

8 *How China spied on the African Union's computers, https://mg.co.za/article/2018-01-29-how-china-spied-on-the-african-unions-computers*

2 Methodology

The research adopted a qualitative approach that included analysis and review of relevant literature on privacy and data protection. Further, policy and legal analysis, as well as conducting key informant interviews with purposively selected respondents were conducted. The research also reviewed reports of previous studies, media reports, academic works, government documents, and other literature. The literature review helped to draw emerging patterns on pertinent privacy and data protection issues and provided guidance on possible sub-themes in relation to the Zimbabwean context.

The study reviewed local laws and policies on privacy and personal data protection, to assess the extent to which they adequately support or protect the enjoyment of the right to privacy. In addition, the study investigated the circumstances under which the laws are variably invoked or interpreted by state and non-state actors to infringe on privacy rights. Such laws and policies include those that govern the telecoms sector, the media, social media, access to information, interception of communications, the role of security and intelligence agencies and security enforcement in general. The study also reviewed relevant international instruments that Zimbabwe is party to and referred to constitutional provisions and draft bills relevant to data protection.

Key informant interviews were conducted with purposively selected respondents drawn from staff of private companies (such as banks, telecoms firms, Internet Service Providers), government ministries (such as those responsible for ICT, security), semi-autonomous bodies (such as electoral commissions, data protection agencies,) telecoms regulators, media houses, social media users, human rights defenders and activists, consumers' associations, academics, lawyers, and select individuals from the general public who were conversant with the issues at hand.

3 Country context

3.1 Political Economy

With a high though debatable[9] unemployment rate[10] and ranking 155 out of 188 countries in the Human Development Index, Zimbabwe is currently classified as a low-income country. The country's population is estimated at 16.9 million persons,[11] the Gross Domestic product (GDP) as of 2017 stood at 2.3%,[12] while the overall poverty rate is projected to increase due to gradual deterioration in economic conditions.

In the run-up to the July 2018 elections, the country was still experiencing a protracted economic crisis exacerbated by the shortage of both US dollars and the local "currency" referred to as "bond notes".[13] Zimbabweans witnessed the return of the concept of 'cash burning',[14] in a whole parallel informal economy where the exchange rate between the USD and the bond go as high as 75%. The dire cash situation led to the over-reliance on mobile money transactions, which became even more apparent when one of the major platforms, Ecocash, crashed for two days, leaving many businesses stranded.[15] There are concerns over the company's dominance in the mobile money sector as it processes about 90% of all local mobile money transactions, with 98% of the country's mobile money subscribers using the platform.[16]

9 *Is Zimbabwe's unemployment rate 4%, 60% or 95%? Why the data is unreliable, https://africacheck.org/reports/is-zimbabwes-unemployment-rate-4-60-or-95-why-the-data-is-unreliable*

10 *The unemployment rate in Zimbabwe is debatable, and depending on who is talking and how they define it, can be as high as 90% or as low as 5%. ZimStat – the official government statistical office – has not conducted a labour survey since 2014, citing "'resource constraints"'. ZimStat last pegged the unemployment rate at around 6% - citing that people in the farming and informal sectors (where majority of Zimbabweans lieare) are considered employed.*

11 *See: http://www.worldometers.info/world-population/zimbabwe-population*

12 *See: http://documents.worldbank.org/curated/en/501001491582965350/pdf/113879-WP-SERIES-AFREC-PUBLIC-4-13-9am-mpo-sm17-zimbabwe-zwe-03-22-17.pdf - Accessed 27 June 2018.*

13 *See: https://www.economist.com/middle-east-and-africa/2017/02/18/zimbabwes-new-bond-notes-are-falling-fast*

14 *" Burning" is a form of selling hard cash on the black market in exchange for a bank transfer or other form of payment at significant percentage*

15 *See: https://11fs.com/blog/zimbabwe-ecocash-crash*

16 *POTRAZ, 2017 4th Quarter Sector Performance report, https://t3n9sm.c2.acecdn.net/wp-content/uploads/2018/03/Sector-Perfomance-report-4th-Quarter-2017-abridged-rev15March2018-1.pdf*

3.2 ICT Status

Zimbabwe currently has three mobile network operators and one fixed line operator. Mobile penetration remains high at 102.7%, while internet penetration is still relatively low at 50.8%. Most Zimbabweans access the internet through their mobile phones. However, mobile internet data bundle costs in the country remains among the highest in the region. There are 16 officially licensed internet service providers, but it is estimated that the total in-country could be more than 28.

There are currently five internet gateways in Zimbabwe: Liquid Telecom (79% market share of equipped bandwidth capacity); TelOne (16,3%); Powertel (2,4%); Dandemutande (1,6%) and Africom (0,6%). TelOne and Powertel are state-owned.[17]

The Postal and Telecommunications Regulatory Authority (POTRAZ) regulates the telecommunications sector and produces a quarterly sector performance report that provides statistics related to internet and telecoms use in the country. According to POTRAZ, nearly half of the internet traffic in Zimbabwe goes to WhatsApp,[18] and this is mainly attributable to the promotional social media access bundles[19] driving up usage on specific platforms.

3.3 Political Environment

Long-time president Robert Mugabe was ousted after 32 years in power in a November 2017 coup, which saw his ally for decades, Emmerson Mnangagwa of the dominant ZANU-PF party, take over as president with the support of the military.[20] Following a July 2018 election, Mnangagwa was declared the winner although the opposition Movement for Democratic Change (MDC) Alliance disputed the poll results.

Technology played a key role in the elections. The Zimbabwe Electoral Commission registered five million voters with a new a biometric system;[21] and while the country was at the peak of the electoral cycle, politicians utilised all types of platforms to get their messages across, including bombarding voters with campaign messages via SMS and WhatsApp groups.[22]

Even after the elections, the ruling party has continued to sharpen its ideological apparatus through deployment of Varakashi[23] – loosely translated as destroyers - following the president's call[24] on his supporters to go onto online platforms and deal with his outspoken online critics.[25]

17 *See: https://www.potraz.gov.zw/images/documents/QReports2016/4th_Quarter_Sector_Performance_Report_Final.pdf*

18 *POTRAZ, 2017 4th Quarter Sector Performance report, https://t3n9sm.c2.acecdn.net/wp-content/uploads/2018/03/Sector-Perfomance-report-4th-Quarter-2017-abridged-rev15March2018-1.pdf*

19 *See: https://www.techzim.co.zw/2017/01/econet-wireless-zimbabwes-new-data-whatsapp-facebook-bundles-prices*

20 *See: https://edition.cnn.com/2017/11/20/africa/zimbabwe-military-takeover-strangest-coup/index.html*

21 *See: http://mobile.apanews.net/en/news/zimbabwe-74-of-eligible-voters-register-to-vote-in-2018-elections*

22 *See: https://www.newsday.co.zw/2018/07/nuisance-campaign-messages*

23 *See: https://www.news24.com/Africa/Zimbabwe/a-vicious-online-propaganda-war-that-includes-fake-news-is-being-waged-in-zimbabwe-20180725*

24 *See: https://twitter.com/Wamagaisa/status/984637362020978689*

25 *See: https://twitter.com/FungaiChiposi/status/990091202577027072*

As the country inched closer to the elections, there were concerns about a possible internet blackout and throttling as has become a trend in many African countries during key national events.[26] With assurances from the ICT Minister,[27] there was no internet blackout in the 2018 electoral cycle. However, there was evidence of TCP/IP blocking of the website zimelection.com by state-owned internet service provider TelOne, following the elections.[28]

26 *At least 11 countries have been documented as having interfered with the Internet during elections: https://qz.com/875729/how-african-governments-blocked-the-internet-to-silence-dissent-in-2016 accessed 20 July 2018.*

27 *See: https://news.pindula.co.zw/2018/06/03/we-will-not-shutdown-internet-social-media-because-of-elections-supa*

28 *See: http://www.dszim.org/2018/08/10/zimbabwean-election-website-blocked-following-2018-general-elections*

4 Laws and Policies Affecting Privacy and Personal Data Protection

This section gives an overview of the policy and legal frameworks for privacy and data protection in Zimbabwe. It also highlights the international, regional and domestic legal framework and their implications on privacy and data protection in the country.

4.1 International Framework for the Protection of Privacy

Zimbabwe has ratified a number of international and regional instruments that provide for the right to privacy and data protection, such as the International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights, Convention on the Rights of the Child,[29] the African Charter on Human and Peoples' Rights.[30] Zimbabwe is also a member of the United Nations General Assembly, thus making provisions of the Universal Declaration of Human Rights binding.[31]

As a state party to the United Nations General Assembly, Zimbabwe has been submitting state reports to the Human Rights Council under the Universal Periodic Review (UPR). However, during Zimbabwe's last UPR session in 2016, there was hardly any mention of commitments regarding data protection and privacy. However, in the Human Rights Council's Working Group on the UPR report on stakeholder submissions on Zimbabwe, it was noted that stakeholders in Zimbabwe had observed that one of the key actions for Zimbabwe was to "ensure that the Data Protection Bill meets international standards and that any data protection authority established by law is appropriately resourced and independent, and has the power to investigate breaches of the data protection principles".[32]

Paragraph 51 of the Human Rights Council's report, on "Right to privacy, marriage and family life", concerns were raised regarding inadequate protection of privacy especially of children. The report specifically noted that "the Committee on the Rights of the Child was concerned about the inadequate enforcement of laws protecting children's right to privacy, in particular in relation to the publication of information by the media relating to children who were either victims of abuse or accused of committing crimes, as well as being subjected to invasive practices such as virginity testing".[33]

29 *See: https://lib.ohchr.org/HRBodies/UPR/Documents/session12/ZW/UNCT-Annex1-eng.pdf*

30 *See: http://www.achpr.org/instruments/achpr/ratification/*

31 *See: https://lib.ohchr.org/HRBodies/UPR/Documents/session12/ZW/ZHRO-JointSubmission3-eng.pdf*

32 *Summary prepared by the Office of the High Commissioner for Human Rights in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21- Twenty-sixth session Of 31 October-11 November 2016*

33 *Compilation prepared by the Office of the United Nations High Commissioner for Human Rights in accordance with paragraph 15 (b) of the annex to Human Rights Council resolution 5/1 and paragraph 5 of the annex to Council resolution 16/21- Zimbabwe*

4.2 National Constitutional Frameworks for the Protection of Privacy

In Zimbabwe, privacy is recognised and protected under the Constitution.[34] Article 57 of the Constitution (as amended) (No.20) Act of 2013, provides for the right to privacy and data protection, as:

> Every person has the right to privacy, which includes the right not to have:
> a. their home, premises or property entered without their permission;
> b. their person, home, premises or property searched;
> c. their possessions seized;
> d. the privacy of their communications infringed; or
> e. their health condition disclosed.

Article 62(3) of the Constitution also provides for the right of persons to have wrong information held by the state about them corrected or deleted, stating that: "Every person has a right to the correction of information, or the deletion of untrue, erroneous or misleading information, which is held by the State or any institution or agency of the government at any level, and which relates to that person".

Besides the constitutional provision, Zimbabwe does not have a specific law on privacy and data protection, but has a number of other laws with provisions expounding on the privacy right and personal data protection such as the Access to Information and Protection of Privacy Act. The Interception of Communications Act on the other hand has provisions that provide for interception of communication, including confiscation of letters.

4.3 Provisions on Personal Data and Privacy in Statutes

4.3.1 The Zimbabwe National Policy for Information, Communications Technology

The most explicit and recent commitments to data protection and privacy are contained in the 2016 Zimbabwe National Policy for Information, Communications Technology, in which the government acknowledges the need for data protection legislative measures such as cyber security laws.[35]

Section 4(f) of the policy statement titled "Policy Absence of Cybersecurity Framework", recognises the importance of data protection within the scope of cybersecurity, noting that "the overall security objective is to ensure the availability, integrity and confidentiality of data in cyberspace".

34 *Constitution of Zimbabwe 2013, http://www.veritaszim.net/node/315*

35 *Zimbabwe National ICT Policy 2016, http://www.ictministry.gov.zw/sites/default/files/Zimbabwe_National_Policy_%20for_ICT_2016-2020.pdf*

Further, the policy makes a commitment to establish a data centre, which amongst other things will be a centralised information storage and protection mechanism. The policy Statement 7.4 [National Data Centre], provides amongst other things that: "The Government of Zimbabwe will establish a national data centre, which allows Zimbabwe to centralise her information storage, management and protection, as well as take advantage of cloud computing opportunities."

Section 19.1, which outlines the policy statement on "E-Commerce Development and Implementation" makes a further commitment which relates to data protection as a critical aspect in e-commerce. Under 19.1(d), the policy statement makes a commitment to "develop, implement and promote appropriate security and legal systems for e-commerce including issues related to cyber security, data protection and e-transactions".

Section 22.1, which outlines the policy statement on the need to "implement Cyber laws and ICT Legislative Provisions," provides that the policy on the enactment of the necessary cyber laws and legislative provisions includes facilitating "the enactment of laws relating to intellectual property rights, data protection and security, freedom of access to information, computer related and cybercrime laws, i.e. Adopt data protection and privacy…" [36]

4.3.2 Access to Information and Protection of Privacy Act [AIPPA][37]

The AIPPA is the closest legislation that Zimbabwe has that provides for privacy and data protection, especially in relation to any information in the custody of public bodies.

Although the law does not specifically refer to "personal data", Section 2 of AIPPA defines "personal information" as "recorded information about an identifiable person, and includes—the person's name, contact details; the person's race, nationality or ethnic origin, colour, religious or political beliefs or associations; age, sex, sexual orientation, marital status or family status; fingerprints, blood type or inheritable characteristics; health care history, including a physical or mental disability; educational, financial, criminal or employment history; anyone else's opinions about the individual; the individual's personal views or opinions, except if they are about someone else; as well as personal correspondence, home and family."

The Act further defines "personal information bank" as "a collection of personal information that is organised or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to that individual and includes personal images".

36 *Policy statement 22.1(d)*

37 *AIPPA available at; https://publicofficialsfinancialdisclosure.worldbank.org/sites/fdl/files/assets/law-library-files/Zimbabwe_Access%20to%20Information%20Law_2008_en.pdf*

Part 5 of the AIPPA provides for the regulation and procedures for collection of personal data by government agencies; including defining purposes for which data may be collected (Section 29). Under section 30(2), public bodies are required to inform the person from whom they intend to collect personal information of the purpose for which the personal information is being collected and the legal authority for collecting it.

Additionally, section 31 requires public bodies intending to use personal information to take every reasonable step to ensure that the information is accurate and complete before use. Section 32 gives data subjects the right to request correction of personal information, while Section 33 requires the head of a public body to protect personal information that is under their custody or control by taking reasonable steps to ensure that there is adequate security and there is no unauthorised access, collection, use, disclosure or disposal of such personal information.

Section 25(1) provides for the protection of personal information to an applicant if the disclosure will result in the unreasonable invasion of a third party's personal privacy. However, this provision is undermined by section 25(2) of the same Act that provides that information may be disclosed where: "the disclosure is desirable or necessary for the purpose of subjecting the activities of the government or a public body to public scrutiny; the disclosure is likely to promote public health and safety or the protection of the environment; the personal information is relevant to a fair determination of the applicant's rights; and the disclosure will assist in researching or validating the claims, disputes or grievances of indigenous people."

4.3.3 Interception of Communications Act[38]

The Interception of Communications Act (ICA) 2007, provides for lawful interception of communication, including seizure of personal possessions such as letters, by authorised persons upon issuance of a warrant for the interception by the Minister of Transport and Communications (Section 5(2). Vesting the powers to issue a warrant in the minister and not the High Court is unfortunate since interception of communications is an infringement of rights and as such, whether this should be permissible in each given case should be a matter for determination by the judiciary which has the capacity to balance competing interests

Section 6(1) of the Act outlines circumstances under which the minister may issue the interception warrants, including gathering information concerning an actual threat to national security, public safety, or national economic interests.

Section 3, however, criminalises unlawful interception, namely interception (without a warrant. It states: "… any person who intentionally intercepts or attempts to intercept, or authorises or procures any other person to intercept or attempt to intercept, at any place, any communication in the course of its occurrence or transmission shall be guilty of an offence and liable to a fine not exceeding level fourteen or to imprisonment for a period not exceeding five years or to both such fine and such imprisonment."

38 *Interception of Communications Act, http://www.vertic.org/media/National%20Legislation/Zimbabwe/ZW_Interception_of_Communications_Act.pdf*

Sections 12(1) and 9(1) of the Act require every service provider to "provide a telecommunications service which has the capacity to be intercepted" and to ensure that "its services are capable of rendering real time and full-time monitoring facilities for the interception of communications," among other duties.

4.3.4 Postal and Telecommunications (subscriber registration) Regulations

In 2013, the government issued the Postal and Telecommunications (subscriber registration) Regulations providing for mandatory SIM card registration, barring any service provider from activating subscriber SIM cards on their telecommunication network system or providing a telecommunication service unless the customer details had been registered and all the requirements complied with.

Per section 4 of the regulations, in order to register a SIM card from a telecommunications provider, a person must produce his or her national identity card or passport and provide personal information, such as full name, permanent residential address, nationality, gender, and subscriber identity number. Where the client is a legal person, they must produce a copy of certificate of registration or incorporation or business licence, among other requirements.

Section 8(3) of the regulations also requires providers "on a monthly basis or at such regular interval as the Authority may from time to time specify" to transmit this information to POTRAZ where it is added to the Central Subscriber Information Database. In 2014, the 2013 regulations were replaced by new regulations that maintain the Central Subscriber Information Database and the penalty of imprisonment of up to six months for failing to register a SIM card or providing incorrect information.[39]

This regulation also requires POTRAZ to appoint data controllers to take responsibility over subscribers' data collected and stored in the Central Subscriber Information Database. The SIM card registration exercise in the country was criticised for undermining the ability of users to communicate anonymously, and because it could facilitate surveillance and make tracking and monitoring of users easier for authorities.[40]

It has been suggested that the consolidated database was inappropriately accessed and used by the ruling party ZANU PF,[41] and doubts linger about the independence and integrity of the telecoms regulator POTRAZ.[42]

---

39 *Privacy International, The Right to Privacy in Zimbabwe, https://privacyinternational.org/advocacy/791/right-privacy-zimbabwe*

40 *"The right to privacy in Zimbabwe, the Digital Society of Zimbabwe, Zimbabwe Human Rights NGO Forum and the International Human Rights Clinic at Harvard Law School, and Privacy International in their "Stakeholder Report Universal Periodic Review 26th Session – Zimbabwe, March 2016*

41 *Access to the consolidated database was to be availed for purposes of law enforcement, upon the written request of a law enforcement agent, or for "safeguarding national security", as well as for "undertaking approved educational and research purposes."*

42 *In the 2013 election year, POTRAZ was placed under the Office of the President and Cabinet and operated under the same for several years.*

4.3.5 National Registration Act[43]

The National Registration Act provides for the registration of persons resident in Zimbabwe and for the issue of identity documents. Under section 6(2) of the Act, applicants for national registration are required to submit documents and provide such information including name and address; citizenship status, birth, entry into Zimbabwe, appearance, marital status, family particulars, tribal affiliations; and registration and liability for National Service in terms of the National Service Act. Finger-prints and photograph are taken, and applicants have to surrender any previously held certificate of registration, registration book or identity card.

Section 8 of the Act requires the Registrar-General and all persons who are employed to conduct the national registration to keep confidential and aid in keeping confidential all information coming to their knowledge in the exercise of their duties. Failure to comply attracts a fine not exceeding level six or to imprisonment for a period not exceeding one year, or both.

4.3.6 Census and Statistics Act [Chapter 10:29][44]

The Act provides for the establishment of the National Statistics Agency as well as for the collection and processing of statistics, among others. Section 17 of the Act prohibits and criminalises the disclosure of data subject information, except for purposes of a prosecution in an offence under this Act. Specifically, Section 17(1) states that: (a) no individual return and no form or answer submitted for the purposes of this Act or any portion of such return, form or answer; and (b) no report or document containing particulars comprised in any such return, form or answer and so arranged as to enable identification of the person by whom or on whose behalf the return was made, form was submitted or answer was given; shall be disclosed to any person who is not employed in carrying out the provisions of this Act, without the permission of the person by whom or on whose behalf the return was made, form was submitted or answer was given.

However, Section 17(3) gives the minister powers to authorise information disclosure. It states: "Notwithstanding anything to the contrary in subsection (1), the Minister may, in writing, authorise the disclosure, on such terms and conditions as he or she may specify in such authority (which terms and conditions must include the prohibition of disclosure of individual information to any person other than the person specified in that authority), of any such individual return, form or answer given to questions put or part of any such return or form or answer, to such person as the Minister shall specify."

---

43 *National Registration Act available at: http://www.parlzim.gov.zw/acts-list/national-registration-act-10-17*

44 *See: http://www.parlzim.gov.zw/acts-list/census-and-statistics-act*

4.3.7 Postal and Telecommunications Act [Chapter 12: 05][45]

The Act has several provisions that prohibit and criminalise privacy breaches and interception of communication, including letters, telegrams and other communications. For example, section 82(1) states that: "Any person authorised to receive or in any way handle any mail or postal article who (b) unlawfully communicates or divulges the contents of any postal article; or (f) without due authority, collects, receives, removes, intercepts or delivers any postal article otherwise than in the ordinary course of his duties …. shall be guilty of an offence and liable to a fine not exceeding level six or to imprisonment for a period not exceeding one year or to both such fine and such imprisonment".

Under section 91(1), employees of a telecommunication licensee or a cellular telecommunication licensee who wilfully intercept or prevent the transmission of a communication commit an offence and are liable to a fine not exceeding level seven or to imprisonment for a period not exceeding two years, or both.

However, the Act also provides for lawful interception of communication, requiring postal or telecommunication licensees or employees in charge of a telegraph office to detain any telegram— (a) which they suspect of containing anything that will afford evidence of the commission of a criminal offence or which they suspect of being sent in order to further the concealment of the commission of a criminal offence; or b) when requested to by a commissioned police officer to detain on the ground that the police officer suspects it of containing evidence of the commission of a criminal offence or that the officer suspects it is being sent in order to conceal the commission of a criminal offence.

4.3.8 Criminal Law Codification and Reform Act

Chapter 8 of the Criminal Law Codification and Reform Act provides for computer-related crimes, including unauthorised access and use of a computer to intentionally destroy or alter, render meaningless, useless or ineffective, copy or transfer, obstruct, intercept, divert, interrupt or interfere with the use of any data, programme or system which is held in a computer or computer network. According to Section 163(1), anyone convicted of this crime will be liable to a fine not exceeding level twelve or imprisonment for a period not exceeding ten years or both.

For purposes of criminalising computer related crimes, section 162 of this Act defines "data" as 'representations of information or concepts that are being prepared or have been prepared for storage or use in a computer…"

45 *See: http://www.parlzim.gov.zw/acts-list/postal-and-telecommunication-services-act-12-02*

4.3.9 Draft Computer Crime and Cybercrime Bill 2017

Zimbabwe is yet to enact a cybercrime law that would deal with cyber related issues and offenses. The Computer Crime and Cybercrime Bill has been in draft form for the last five years and there is no clarity on when it might be passed. It is the only piece of legislation that has general provisions regarding breach of information collected in terms of various regulations, even though the provisions are not restricted to cyber incidents. The Bill creates offences related to data breaches which include unlawful access, unlawful interception of data, unlawful data acquisition, and unlawful interference with data or data storage medium. It also criminalises the sending of unsolicited electronic messages (referred to as spam), and criminalises the non-consensual distribution of intimate images.[46] Further, it provides for a 'Cybersecurity Centre' which would, among other purposes, act as a response mechanism for cyber incidents.

46 *See: https://www.herald.co.zw/revenge-porn-law-long-overdue*

5 Results: Status, Trends and Challenges

This section presents the emerging trends and key challenges to privacy and personal data protection in Zimbabwe, citing various examples and incidents.

5.1 Limited Understanding of Privacy

Study findings show that privacy still is not a big issue for a lot of Zimbabweans, who genuinely think they have nothing to hide when they hear about a facial recognition program or a mandatory SIM card registration initiative. In Zimbabwe, there is also no direct translation or equivalent term for the word "privacy". For example, in Shona, a language widely spoken in Zimbabwe, the closest words are 'chakavandika' or 'tsindidzo' which, though hardly used in normal conversations, mean secret.

This lack of understanding and apathy could also be partly because the government has historically managed to make citizens believe that the introduction of intrusive technologies and processes is entirely for the public good. A previous perceptions research study also showed that although a majority of Zimbabweans considered privacy a human right and a thing to be respected, popular belief was that privacy was limited to privacy of communications, mostly via telephone and email.[47] None of the respondents immediately thought of privacy in terms of collection, storage and processing of biometric data.

According to a 2014 research study on the perceptions on the right to privacy in Zimbabwe, "when people operate in an economy where they daily grapple with cash shortages, unemployment and how to keep body and soul together, things like rights to privacy take a backseat or occupy the bottom rung in their pecking order of priorities."[48]

47 *See: https://www.academia.edu/11846294/Public_Perceptions_of_the_Right_to_Privacy_in_Zimbabwe*

48 *Interview held with key informant on 23 July 2018*

5.2 Weak Policy and Legal Frameworks

5.2.1 Absence of Comprehensive Data Protection Frameworks

Zimbabwe is yet to enact a comprehensive privacy and data protection law to regulate the collection, processing and sharing of user personal data and provide remedies for redress of violations of privacy of personal data. The main piece of legislation that remotely provides for privacy and data protection is the Access to Information and Protection of Privacy Act (AIPPA) – whose provisions may not be adequate to address the many emerging issues especially in a digital era, where there is massive collection and sharing of personal information. For instance, if citizens wanted to seek redress for the unsolicited campaign SMSes they received, or to seek answers on how their phone numbers were obtained, AIPPA would be useless because it applies the right of access is only applicable to information that is held by public bodies.

The absence of a unified data protection regulation is particularly of concern following the launch of the country's 'first data centre' by the (government-owned) fixed telecommunications company, TelOne, in March 2017.[49]

There have been efforts to enact laws that would enhance privacy and data protection such as the Computer Crime and Cybercrimes Bill and the Data Protection and Electronic Transaction Bills that remain under discussion. However, there appears to be a lack of clear policy direction. This is particularly so considering the length of time that has passed without their finalisation and passage into law as well as the number of times that the Bills have been changed. For example, the Computer Crime and Cybercrime Bill is now in its third draft version. The longer it takes to pass these laws, the longer the gaps in the protection of these rights will persist.

5.2.2 Limitations on the Right to Privacy

Despite the constitutional provisions, the right to privacy faces limitations, specifically section 86(1) which among other things provides that the fundamental rights (including the right to privacy) and freedoms must be exercised reasonably and with due regard for the rights and freedoms of other persons. Section 86(2) provides that the limitations must only be applied to the extent that they are "fair, reasonable, necessary and justifiable in a democratic society based on openness, justice, human dignity, equality and freedom, taking into account all relevant factors."

Unfortunately, the right to privacy is explicitly limited under the subsequent legislation such as the AIPPA and the Interception of Communications Act. Section 25 of AIPPA provides that information may be disclosed in some instances, such as where the disclosure is desirable or necessary for the purpose of subjecting the activities of the government to public scrutiny, and to promote public health and safety. Moreover, Section 6(1) of Zimbabwe's Interception of Communications Act outlines circumstances under which privacy and data protection may be restricted by allowing for the issuance of warrants to intercept communications in specific circumstances.[50]

49 *See: https://www.dailynews.co.zw/articles/2017/03/27/telone-unveils-zim-s-first-data-centre*

50 *Interception of Communications Act https://bit.ly/R5gPZO*

5.2.3 Abuse of the Laws to Undermine Privacy

There have been several instances where law enforcement agencies have flouted existing legislation in ways that undermine privacy. For example, in July 2011, a court order was granted for police to search and seize the cell phone records belonging to then Minister of Finance Tendai Biti, as part of their investigations in a case of alleged corruption. A warrant was issued by the Magistrates Court ordering the mobile phone operator Econet to release the minister's cell phone records, which the minister contested at the High Court.[51] The police went on to make an urgent application for a search warrant in terms of sections 49 and 50 of the Criminal Procedure and Evidence Act (CPEA) to authorise them to enter the minister's premises and to seize the required call history records. In determining the appeal against the warrant to search his communication, the High Court held that while Biti had a constitutionally guaranteed right of privacy, it was not absolute and could be limited by the police's right to investigate where there was reasonable cause and it was in the public interest to do so. On that basis, it dismissed Biti's application for an injunction against police accessing his call records.

However, the frequency of warrants or court orders cannot be stated with certainty because in most cases, the warrants for interception are not made public. There is therefore a possibility that warrants of interception are issued and that monitoring and interception is on-going in several cases outside of the public eye.

5.2.4 Legal Provisions Compelling Telecom Companies to Cooperate on Surveillance

Section 12(1)a of the Interception of Communications Act requires telecommunications service providers to put in place equipment with capabilities for interception of communications as part of their licensing conditions. The Act requires that before a telecommunications company enters a contract with a subscriber, it must obtain specific information including names, addresses, copies of identity documents and proof of residence, among other things.

The Act specifically allows for the interception of verbal and audio conversations as well as the reading and copying of postal communications. The Act does not provide clear definitions of the term communications "monitoring", leaving room for the interception of means of communication that are currently not established.[53]

---

51 *Biti v Majuta and Others – (HC 6608/11) [2011] ZWHHC 156(12*

52 *See: https://www.ohchr.org/Documents/Issues/Privacy/ZimbabweHumanRightsForum.pdf*

53 *Ibid*

5.3 Data Collection Programmes by Zimbabwe

Over the past few years, the Zimbabwean government has implemented several initiatives that have required mandatory collection and processing of personal data. These have included the SIM card registration, which was introduced in 2010 although the regulations, the Postal and Telecommunications (subscriber registration) Regulations, were only passed in 2013 with amendments made in 2014. The regulations require collection of specified data from all persons as a precondition for registration with and receipt of services from telecommunication service providers.[54]

The data to be collected includes names, addresses, gender and national identification numbers. The law requires telecom operators to regularly provide copies of this data to the government, which enabled the government to create its own central subscriber information database. Penalties for non-compliance include possible revocation of the service provider's operating license.

Besides concerns that the ruling party may have accessed data from the Central Subscriber Information Database, the SIM card registration exercise was criticised for undermining the ability of users to communicate anonymously, and because it could facilitate surveillance and make it easier for authorities to track and monitor users.[55]

Another mandatory data collection exercise was launched in 2017, when the Zimbabwe Electoral Commission introduced the Biometric Voter Registration system for voter registration. This saw the collection of personal information such as mobile numbers, photos and physical addresses of at least five million registered voters.[56]

54 *Section 4(1)*

55 *"The right to privacy in Zimbabwe, the Digital Society of Zimbabwe, Zimbabwe Human Rights NGO Forum and the International Human Rights Clinic at Harvard Law School, and Privacy International in their "Stakeholder Report Universal Periodic Review 26th Session – Zimbabwe, March 2016*

56 *See: http://mobile.apanews.net/en/news/zimbabwe-74-of-eligible-voters-register-to-vote-in-2018-elections*

5.4 Risk factors

The most pertinent concerns on privacy and data protection in Zimbabwe are that ordinary citizens have a limited understanding of this right, and that there is low political will to either update existing laws to recognise these rights, or to pass a new law addressing these rights. The Computer Crime and Cybercrime Bill that has been in the pipeline for the past five years. At the same time, the Bill is highly flawed and deficient in a context where the drafters lack the will to meaningfully involve stakeholders in its drafting.

This research has highlighted how people in positions of authority tend to abuse their roles in terms of accessing personal data, as has been seen with the recent ZANU PF SMS scandal. There are widespread beliefs among Zimbabweans that telecom companies are in the business of selling subscribers' phone numbers to businesses that advertise through bulk SMS. Because there is generally not a culture within governmental and non-governmental bodies to explain why they collect certain information, it is less apparent to many people when personal data other than what is relevant or required for the service they seek is collected.

All the non-governmental bodies interviewed highlighted their awareness of risks of breaches. Although most of the non-governmental bodies have privacy policies, they do not necessarily adhere to international standards, particularly due to lack of guidance from relevant local legislation or standard regulations. Most of their policies stipulate the kind of data collected and how it is used, but rarely specify under what circumstances data would be shared.

On the other hand, banks highlighted that training staff on privacy and data protection awareness was their top priority, especially in a context of internet banking where cybercrime is rife. They also have security teams that do regular monitoring of security systems and mechanisms. Physical copies of data in banks tend to be kept for up to five years, according to the money laundering law. All the interviewed bodies said they had mechanisms of testing the effectiveness of their data protection controls.

5.5 Enhanced State Surveillance Capacity

In March 2018, the government signed a deal for a strategic partnership with the Guangzhou-based start-up, CloudWalk Technology, to begin a large-scale facial recognition program throughout the country.[57] Although the project was touted as intended to help the government build smart financial services and fight crime, it was established[58] that the main purpose of the project was that China needed black faces to help it "train the racial bias out of its facial recognition systems".[59] Most important was that the government would build a national facial database, and then share it with the Chinese government. There are fears that through this project, the government would significantly improve its capacity to conduct mass surveillance.

This is not the first time the government has entered deals of this nature that are intended to surveil citizens. In 2015, then president Robert Mugabe received a "gift"[60] from Iran in the form of various cyber-surveillance technologies, including International Mobile Subscriber Identity (IMSI) catchers.[61] With both deals, there was utter disregard for the opinions of rights experts and the people on whom the invasive technologies would be used.

5.6 Targeted and Indiscriminate Communication

Zimbabweans have always received unsolicited SMS, and apart from these being a petty annoyance, they have been protected by a law requiring bodies that use such means to avail and advertise an option to opt out.

At the height of the 2018 electoral campaigns, the ruling party, ZANU PF, is alleged to have obtained the phone numbers of registered voters and blasted personalised campaign messages to them in violation of their privacy.[62] The sending of unsolicited campaign messages was not only frowned upon for their annoyance but raised questions about the security of citizens' information. Following a public outcry over this abuse of personal information, ZANU PF claimed that the SMS had been sent only to their members.[63] However, this was not true as independent and opposition candidates also received the messages. Moreover, the fact that citizens not registered to vote did not receive the SMS suggests that ZANU PF had access to the ZEC databases containing people's names, their mobile numbers, and constituency information.

---

57 *See: http://www.globaltimes.cn/content/1097747.shtml*

58 *See: https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/?utm_source=PostUp&utm_medium=email&utm_campaign=Editors%20Picks%20%207/24/2018%20-%20BSA&utm_keyword=Editor%27s%20Picks%20OC*

59 *Studies have shown that popular facial recognition technologies have a high error rate when attempting to identify the gender of dark skinned people. The accuracy of artificial intelligence (AI) depends on the data it is fed, and, worldwide, facial recognition AI has been trained on predominantly white and male faces.*

60 *See: https://bulawayo24.com/index-id-news-sc-national-byo-61558-article-iran+gives+mugabe+spy-technology.html*

61 *Telephony eavesdropping devices used for intercepting mobile phone traffic and tracking movement of mobile phone users*

62 *https://bulawayo24.com/index-id-news-sc-national-byo-140387.html*

63 *See: http://businesstimes.co.zw/zanu-pf-admits-sending-out-bulk-sms*

.

Further, there were reports that Mobile Network Operators (MNOs) offered their subscriber databases for use by ZANU PF.[64] There were suggestions that ZANU PF could access the information once the centralised mobile subscribers' database was created following the introduction of mandatory SIM card registration.

Ironically, Section 21(9) (b) of the Electoral Act criminalises the misuse of personal information contained on the voters' roll. It stipulates that anyone who makes use of the voters' roll for commercial or other purposes unconnected with an election shall be guilty of an offence and liable to a fine or jail term not exceeding five years or to both a fine and imprisonment.

5. 7 Dispute Resolution and Remedies

Section 8(13) of the Postal and Telecommunications (Subscriber) Regulations grants anyone aggrieved by the unlawful use of their personal data the right to seek legal redress. Under section 18 of the Interception of Communications Act, a person aggrieved by a warrant or directive relating to interception of communications, may appeal to the Administrative Court within one month of being notified or becoming aware of it. The court may confirm, vary or set aside the warrant, directive or order. However, given that interception is usually done without the knowledge of the subject, it is difficult to know if there has been a breach.

The AIPPA also provides for an internal remedy mechanism before recourse can be had to the courts. Section 53 provides for reviews relating to collection or correction of personal information amongst other reviews, to be made to the Zimbabwe Media Commission. However, recourse to this body has been of public contention since the coming into force of this law. This is because the Commission is loaded with multiple regulatory roles such as information requests as well as media regulation matters. Also, its mandate relating to protection of privacy and data protection is very limited. Moreover, this Commission has had no commissioners since 2015, when the terms of the previous commissioners expired. Although interviews for new commissioners were conducted, no appointments have been made, and the government has not given reasons for the delay.[65]

64 *All MNOs issued statements refuting granting access to their subscriber databases by Zanu PF, but they confirmed sharing unspecified data that they describe as 'only relevant information' with the regulatory authority, that is POTRAZ. See also: https://zimmagazine.com/econet-refutes-zecs-claims-that-it-sold-its-database-to-zanu-pf-after-voters-roll-details-leak*

65 *Zimbabwe Independent, Misa sounds warning https://www.theindependent.co.zw/2018/06/15/misa-sounds-warning/*

5.8 Progressive Steps Towards Data Protection

There have not been any notable positive developments on the front of privacy and data protection in the country. One development is the fact that AIPPA makes provision for the establishment of a data protection bill that would govern both private and public bodies. If enacted, the law would "provide for the regulation of data protection" and enable the establishment of a data protection authority.

Civil society has also been involved in the push for the recognition of privacy and data protection in the country. This has either been through reviews of the draft Computer Crime and Cybercrime bill by making submissions to relevant parliamentary portfolio committees. Following the ZANU PF SMS scandal, there was a public outcry for the electoral commission to omit voters' pictures from the final roll that they released to parties, due to the potential threat associated with indiscriminate sharing of people's personally identifiable data.[66]

66 *See: http://kubatana.net/2018/07/12/opposition-political-parties-pro-democracy-campaigners-team-challenge-bid-stop-zec-releasing-voters-roll-photographs*

6 Conclusion and Recommendations

6.1 Conclusion

The lack of clear regulation and consolidated legislation on the privacy and personal data protection front presents a myriad of risks and challenges for Zimbabweans. The blatant abuse of people's personal information, in the absence of a clear authority charged with the responsibility to deliver remedies for people or to advocate for their rights when they have been infringed, remains a challenge. The situation is worsened when it is the state or well-placed powerful entities committing these violations and there being no means to hold them accountable. It is also clear that in a context riddled with political and economic difficulties, the public are more concerned with immediate issues of bread and butter than what they consider to be less tangible issues, such as privacy and data protection.

There are documented efforts of civil society making written and verbal submissions to legislators, concerning privacy and data protection. However, the current attitudes of the lawmakers are that of exclusion and disdain. To some extent, civil society efforts have resulted in some submissions being taken on board. For example, after massive lobbying[67] by women's rights groups, revenge porn was recognised as a form of gender-based violence, leading to its criminalisation in the Computer Crime and Cybercrime bill.

67 *See: https://www.techzim.co.zw/2016/03/revenge-porn-laws-zimbabwe-parliament-petition*

6.2 Recommendations

Government

- Prioritise the finalisation of the country's cyber security legislation. The government can also learn from the developments in European Union's General Data Protection Regulation (GDPR), which provides a useful starting point and template for the country to craft its cyber laws and data protection regulations.
- Speed up adopting the African Union Convention on Cybersecurity and Personal Data Protection (also referred to as the Malabo Convention) - the first pan-African guiding instrument on privacy and personal data protection on the continent.
- Meaningfully involve multi-stakeholders including civil society, academia and the private sector crafting rights-respecting and effective data protection laws.
- Re-align existing privacy laws with the constitution so as to restore the confidence of citizens in governance processes related to data protection.

Private Companies

- Develop privacy policies that are distinct and easy to locate on their websites and do not have to wait for or depend on national legislation to create and abide by rights-respecting privacy policies.
- Respect and protect privacy rights as a moral obligation regardless of the duties imposed upon them by the state, including committing to push back on inappropriate or overly broad information requests made by the government or other bodies.
- Train staff and conduct other relevant internal activities aimed at improving the protection of data and privacy.
- Implement the recommendations of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, which call on companies to "seek to prevent or mitigate the adverse human rights impact of their involvement to the maximum extent allowed by law".[68]
- Take all necessary and lawful measures to ensure that they do not cause, contribute to or become complicit in human rights abuses.

Media

- Raise the awareness among the public of privacy and data protection issues, by reporting objectively and informatively on developments in these areas.

---

68 *See: http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/35/22*

Technical Community

- Increase their involvement in processes that seek to influence the development and implementation of data protection laws.
- Offer useful solutions to lawmakers who are often not well versed with the technicalities surrounding these issues.

Civil Society Actors

- Work to enhance the capacity of citizens to understand privacy and data protection issues, as well as how and why to demand rights-respecting legislation.

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Plot 6 Semawata Place, Ntinda, P.O Box 4365 Kampala, Uganda.
Tel: +256 414 289 502| Mobile: +256 790 860 084, +256 712 204 335
Email: programmes@cipesa.org
Twitter: @cipesaug
Facebook: facebook.com/cipesaug
www.cipesa.org