The Right to Privacy, Interception of Communications and Surveillance in Zimbabwe [1]

1. **INTRODUCTION**

1.1. The Constitution of Zimbabwe provides for the right to privacy i.e the right not to have one's home, premises or property entered without their permission; their person, home or premises or property searched; their possessions seized; the privacy of their communications infringed; or their health condition disclosed;[2]

1.2. It does not however provide in clear and unequivocal terms a protection against being the subject of physical and other surveillance in the form of espionage and same must be inferred or read into the above protection. That is the approach taken in this paper;

1.3. The right to privacy aforementioned is however not absolute and is subject the Limitations Clauses of the same Constitution which require, among other things, for the exercise of the right to privacy to be "exercised reasonably and with due regard for the rights and freedoms of other persons."[3]

1.4. The State and even other private institutions and persons routinely subject citizens to all manner of invasion of privacy by way of either interception of communications and or surveillance for various reasons that include but are not limited to security, marketing and other legal duties;

1.5. In Zimbabwe, there exists the legal framework for the protection of privacy as well as for the lawful invasion of privacy by way of either interception of communications and or surveillance and the latter is aimed mostly at the detection, investigation and prevention of criminal and or civil wrongs in the physical realm;

1.6. With the onset and advancement of information communication technology, said criminal and civil wrongs have also transcended the physical realm to the cyberspace and so has the surveillance of conduct and the interception of communications;

1.7. The purpose of this discussion paper is to survey the phenomenon of interception of communications and surveillance in Zimbabwe as measured against the constitutional right to privacy and regional and international best practices.

2. THE CONSTITUTIONAL AND LEGAL BASES FOR THE PROTECTION OF PRIVACY AND PREVENTION OF EITHER SURVEILLANCE AND OR INTERCEPTION OF COMMUNICATIONS

2.1. Section 57 of the Constitution of Zimbabwe, *supra* is the constitutional basis for the protection of privacy;

2.2. The Constitution sets out a fairly high standard for the limitation of rights in general, applicable in equal measure to the right to privacy in the following terms:

"The fundamental rights and freedoms set out in this Chapter may be limited only in terms **of a law of general application** and to the extent that the limitation is **fair, reasonable, necessary and justifiable** in a democratic society based on openness, justice, human dignity, equality and freedom taking into account all relevant factors including –

(a) The nature of the right or freedom concerned;

(b) The purpose of the limitation, in particular whether it is necessary in the interests of defence, public safety, public order, public morality, public health, regional or town planning or the general public interest;

(c) The nature or extent of the limitation;

(d) The need to ensure that the enjoyment of rights and freedoms by any person does not prejudice the rights and freedoms of others;

(e) The relationship between the limitation and its purpose, in particular whether it imposes greater restrictions on the right or freedom concerned than are necessary to achieve its purpose; and whether there are any less restrictive means of achieving the purpose of the limitation."[4]

2.3. The right to privacy, like other rights except the right to life, human dignity, freedom from torture, cruel, inhuman or degrading treatment or punishment, freedom from slavery or servitude, fair trial and *harbeus corpus,* "**may be further limited by a written law providing for measures to deal with situations arising during a period of public emergency, but only to the extent permitted by this section and the Second Schedule."** [5]

2.4. It is against the foregoing background that the State and other persons routinely engage in permissible invasion of the privacy of citizens by way of either surveillance and or interception of communications;

2.5. Such invasion of privacy by way of either surveillance and or interception of communications is typically grounded in laws such as the select examples below;

2.6. <u>Access to Information and Protection of Privacy Act [*Chapter 10:*27]</u>

2.6.1. The protection of privacy, together with the constitutional limitations attendant to it, presently find further expression in the Access to Information and Protection of Privacy Act [*Chapter 10:27*][6] which is an Act of Parliament meant to "provide members of the public with a right of access to records and information held by public bodies; to make public bodies accountable by giving the public a right to request correction of misrepresented personal information; to prevent the unauthorised collection, use or disclosure of personal information by public bodies; <u>to protect personal privacy</u>…"[7]

2.6.2. Aside from creating a right to access only to information held by public bodies in line with Section 62 of the Constitution, and most importantly for purposes of this discussion, this Act provides a substantive right to the protection of personal privacy by, among other things, prohibiting unauthorised collection, use or disclosure of personal information by those public bodies;

2.6.3. It is notable that the right to personal privacy provided for by the Act is restricted to the interaction of persons only with public bodies and does not extend to other private persons and or entities;

2.6.4. The Act protects personal privacy and personal information more particularly as follows:

2.6.5. "personal information" for purposes of the Act and the protection thereof is defined to mean "recorded information about an identifiable person, and includes—the person's name, address or telephone number; the person's race, national or ethnic origin, colour, religious or political beliefs or associations; the person's age, sex, sexual orientation, marital status or family status; an identifying number, symbol or other particulars assigned to that person; fingerprints, blood type or inheritable characteristics; information about a person's health care history, including a physical or mental disability; information about educational, financial, criminal or employment history; anyone else's opinions about the individual; and the individual's personal

views or opinions, except if they are about someone else; personal correspondence, home and family;"[8]

2.6.6. The Act prescribes the very limited purposes for which a public body may collect personal information and these are only where the collection is prescribed by law; the information is to be collected for the purposes of national security, public order and law enforcement; or the information is to be collected for the purposes of public health; or the information relates directly to and is necessary for an operating programme, function or activity of the public body; or the information will be used to formulate public policy;[9]

2.6.7. The Act then prescribes that a public body must collect personal information from the individual concerned personally;

2.6.8. The only exceptions or instances where a public body may collect information indirectly or from third parties or surveillance is if the individual concerned consents to such collection of information, or the public body is authorized by the Zimbabwe Media Commission or the collection is authorized by another law in force in Zimbabwe; or the information is collected for purposes of determining the suitability for granting an honour or award, including an honorary degree, scholarship, prize or bursary; or proceedings before a court or judicial or quasi-judicial tribunal; or collecting a debt or fine or making a payment; or law enforcement;[10]

2.6.9. The individual data subject of the collection of information is entitled as of right to be advised of the fact of and the purpose of the collection of the personal information and the legal basis for doing so except where the Zimbabwe Media Commission authorises the public body not to disclose the said fact and or authority or where to advise the data subject would prejudice law enforcement and or the purpose of the data collection;[11]

2.6.10. The Act casts a duty on every head of a public body to protect personal information that is under his 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;[12]

2.6.11. Personal information collected by a public body may only be used for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose or otherwise with the consent of the data subject;[13]

2.6.12. The National Archives, or the archives of a public body, may disclose personal information for archival or historical purposes if such disclosure would not result in an unreasonable invasion of a person's personal privacy in terms of this Act; or the information is about a person who has been deceased for thirty or more years;[14]

2.7. **Criminal Procedure and Evidence Act [*Chapter 9:07*]**

2.7.1. This is the law that regulates the criminal justice system of Zimbabwe regarding the investigation, detection, arrest, and prosecution of and punishment for crime;

2.7.2. By way of example, a number of serious offences are routinely prosecuted on the strength of evidence obtained from closed circuit camera surveillance footage;[15]

2.7.3. The elements of surveillance in this regard include but are not limited to the routine and sometimes random stop and search procedures conducted by the police on roads and in motor vehicles across Zimbabwe;[16]

2.7.4. Routine profiling of individuals after arrest and conviction is also surveillance;

2.7.5. The intelligence services also routinely profile individuals and organisations alike in the name of state security;

2.7.6. Most court records of criminal convictions are regarded as public information available for inspection;

2.7.7. The law of evidence provides for the compulsion of the disclosure of what may be confidential information during criminal trials such as by way of an order for medical or mental health examination of either suspects and or witnesses in terms of either the Criminal Procedure and Evidence Act [*Chapter 9:07*] itself or the Mental Health Act [*Chapter 15:12*]

2.8. **Civil Evidence Act [*Chapter 8:01*]**

2.8.1. This is the law that regulates the civil justice system of Zimbabwe regarding the collection, treatment and admissibility of evidence in civil matters such as contractual disputes, family law disputes and other matters not regulated by the criminal law;

2.8.2. The elements of surveillance in this regard include but are not limited to the conducting of civil trials in public and the preservation and accessibility of civil court records;

2.8.3. Most court records of the outcomes of civil dispute resolution proceedings are regarded as public information available for inspection;[17]

2.9. **Interception of Communications Act [*Chapter 11:20*]**

2.9.1. This Act outlaws the interception or surveillance of communications other than in accordance with the provisions of the Act itself;[18]

2.9.2. Any evidence obtained by way on an unlawful interception or surveillance of communication is not admissible evidence in a criminal trial;[19]

2.9.3. It further provides for the circumstances in which the interception or surveillance of communications is lawful such as when the person intercepting the communication is a party to the communication, or the communication is intercepted with the consent of the recipient or sender of the communication, or where there is a warrant for such interception or surveillance;

2.9.4. The act then lays out the procedure for the application of an interception or surveillance of communication warrant by authorized persons which is made to a Minister upon showing the required circumstances for its issue;

2.9.5. An interception warrant may be issued and is valid for three months if there are reasonable grounds for the Minister to believe that a serious offence by an organised criminal group has been or is being or will probably be committed, or that an offence referred to in the Third Schedule[20] or in paragraph 1, 2, 3, 4, 5, 6, 7 or 8 of the Ninth Schedule[21] to the Criminal Procedure and Evidence Act [*Chapter 9:07*] has been or is being or will probably be committed , or for the gathering of information concerning an actual threat to national security or to any compelling national economic interest, or for gathering of information concerning a potential threat to public safety or national security;

2.9.6. The Minister may issue any directive to a service provider not involving any interception or monitoring of communications, instead of issuing a warrant;

2.9.7. The Minister may likewise amend, revoke and or extend any warrant issued;

2.9.8. Extensions of warrants are for three months and thereafter any further extensions may be made by way of *ex parte* application to the Administrative Court of Zimbabwe by the authorised person seeking such extension;

2.9.9. Persons authorized to apply for interception warrants are limited to the Chief of Defence Intelligence or his or her nominee; the Director-General of the President's department responsible for national security or his or her nominee; the Commissioner General of the Zimbabwe Republic Police or his or her nominee; and the Commissioner General of the Zimbabwe Revenue Authority or his or her nominee.[22]

2.9.10. An application for an interception warrant must identify the person or customer, if known, whose communication is required to be intercepted; and the service provider to whom the direction to intercept the communication must be addressed, if applicable; and the nature and location of the facilities from which, or the place at which, the communication is to be intercepted, if known; and full particulars of all the facts and circumstances alleged by the applicant in support of his or her application; and whether other investigative procedures have been applied and have failed to produce the required evidence, or the reason why other investigative procedures appear to be unlikely to succeed if applied, or whether they involve undue risk to the safety of members of the public or to those wishing to obtain the required evidence; the period for which the warrant is required to be issued; and the basis for believing that communication relating to the ground on which the application is made will be obtained through the interception; and any other information which may be required by the Minister for the Minister to make an appropriate decision;

2.9.11. A Monitoring of Interception of Communications Centre (MICC) is established by the Act for purposes of carrying out lawful interceptions;[23]

2.9.12. All information communication technology service providers are under a legal obligation to gather data of their users and customers and to give access to authorised persons to intercept and or survey communications. In fact their equipment and technology is mandated by law to have capabilities for interception in accordance with the Act;[24]

2.9.13. Authorised persons are permitted to issue disclosure notices to persons reasonably suspected of having communications and or information liable to interception and failure to disclose or give access to such information and or communication attracts criminal liability punishable by a ZW$30,000.00 fine and or imprisonment;[25]

2.9.14. Postal articles reasonably suspected to be capable of interception and or surveillance are subject to the power of the Minister to issue detention order of the postal articles;[26]

2.9.15. All persons who have access to information and or communications or postal articles in terms of the Act are under a duty of confidentiality and not to disclose to any other person other than in circumstances authorised by the Act;[27]

2.9.16. An unlawful disclosure of information, communication and or postal article acquired in terms of the Act attracts criminal liability and is also punishable by a ZW$30,000.00 fine and or five term of imprisonment;[28]

2.9.17. Material obtained in terms of the Act must be destroyed as soon as possible after it has been used;[29]

2.9.18. Any person aggrieved by any exercise of power whether by way of warrant, directive and or detention order in terms of the Act may appeal within one month of the conduct complained against to the Administrative Court of Zimbabwe;[30]

2.9.19. The Minister responsible for the Act has to report annually to the Attorney General of Zimbabwe on the instances where the provisions of the Act have been used;[31]

2.9.20. The Minister may make further regulations for the operation of the powers in the Act;[32]

3. **Comparative Legal Frameworks**

3.1. **The Telecommunications (Interception and Access) Act, 1979, the Surveillances Devices Act, 2004 and the Telecommunications Act, 1997 of Australia**

3.1.1. The Department of Home Affairs administers the two laws;

3.1.2. The former Act protects the privacy of Australians by prohibiting interception of communications and access to stored communications;

3.1.3. The privacy of Australians is also protected by the Telecommunications Act 1997, which prohibits telecommunications service providers from disclosing information about their customers' use of telecommunications services;

3.1.4. The TIA Act sets out certain exceptions to these prohibitions to permit eligible Australian law enforcement and security agencies to:

3.1.4.1. obtain warrants to intercept communications;

3.1.4.2. obtain warrants to access stored communications;

3.1.4.3. authorise the disclosure of data

3.1.5. Agencies can only obtain warrants or give authorisations for national security or law enforcement purposes set out in the TIA Act;

3.1.6. The SD Act governs the use of surveillance devices by agencies;

3.1.7. Under the SD Act, an eligible agency can apply for a warrant to use a surveillance device to investigate a relevant offence;

3.1.8. Although the Department of Home Affairs administers the TIA Act and SD Act, the department does not investigate crimes.[33]

3.3. **The Regulation of Interception of Communications and Provision of Communication – Related Information Act 70 of 2002 (RICA); National Strategic Intelligence Act 30 of 1994 (NSI) , and the Intelligence Services Control Act 40 of 1994, South Africa**

3.3.1. This law, likewise permits the interception of communications of any person by prescribed authorized officials of the State and subject to prescribed conditions;

3.3.2. Key in the South African interception framework is the appointment, by the Minister, of a Designated Judge to consider any and all applications for interceptions and or directives concerning information;

3.3.3. The South African law has been undergoing considerable revision efforts which may lead to a complete overhaul of the entire RICA if sentiments placed on record in the High Court and Parliament are anything to go by;

3.3.4. More importantly, and as recently as 16th September 2019, a South African Court condemned and struck down or otherwise amended key provisions of the RICA more particularly as follows:

3.3.4.1. Where the Act did not provide for post – interception notice to data subjects, the Court found such provisions to be inconsistent with the South African Constitution by failing to provide adequate safeguards against abuse and to prevent the possibility of data subjects never ever being able to know that they had been the subjects of information interception;[34]

3.3.4.2. Where the Act provides for the appointment of a designated judge by the Minister, the Court retained that power but with the qualification that "**however, the appointees should be nominated by the Chief Justice and the Minister should be obliged to accept the nominations."[35]**

3.3.4.3. The Court declined to rule in favour of a prayer to introduce the institution of a public advocate to act as a further safeguard in applications for interception warrants as part of the adversarial system of litigation. Whilst noting that such an institution may be a safeguard given the *ex parte* nature of all applications for interception it was content to declare the relevant provision as *ultra vires* the Constitution but without prescribing the manner of curing the defect and left it to the legislature to do so in within two years of its order; [36]

3.3.4.4. The Court declined to outlaw the provisions regarding archiving and storage of intercepted information and contented itself with ordering a revision of the weak safety measures regarding the control, access to and dissemination of such stored information in the following terms:

"(1) RICA, especially sections 35 and 37, are inconsistent with the Constitution and accordingly invalid to the extent that the statute, itself, fails to prescribe proper procedures

to be followed when state officials are examining, copying, sharing, sorting through, using, destroying and/or storing the data obtained from interceptions;

(2) The declaration of invalidity is suspended for two years to allow Parliament to cure the defects."[37]

3.3.4.5. When presented with the case for stronger protection against the interception of lawyer – client and journalist – source information, the Court again contented itself in respect of lawyers but attacked the inadequacies of the protection of journalists and their sources as follows:

"[140] In my view the absence of express provisions enjoining the designated judge to examine the justification of spying on a journalist is evidence of a failure to align RJCA with section 16(1) rights. The absence renders RJCA in that respect, unconstitutional."

3.4. **Interception of Communications Act [*Chapter 15:08*] of Trinidad and Tobago**

3.4.1. The Act interestingly starts off by making the bald declaration that it is *ultra vires* the Constitution of Trinidad and Tobago which Constitution ironically[38] allows for the enactment of unconstitutional laws as long as there is, in the legislation an acknowledgement of the said unconstitutionality;

3.4.2. Like the Zimbabwean Act, this Act seeks to "provide for and about the interception of communications, the acquisition and disclosure of data relating to communications, the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed and other related matters."[39]

3.4.3. The definition of "communication" which may be intercepted is broader and well articulated in the following terms:

"communications" includes anything comprising speech, music, sounds, visual images or data of any description or signals between persons, between a person and a thing or between things or for the actuation or control of any apparatus, and whether or not done in real time; "intercept", in relation to a communication, means listening to, monitoring, viewing, reading or recording, by any means, such a communication in its passage over a telecommunications network without the knowledge of the person making or receiving the communication"

3.4.4. The definition of "interception" | surveillance is, likewise, broader and much better articulated in the following terms:

"intercept", in relation to a communication, means listening to, monitoring, viewing, reading or recording, by any means, such a communication in its passage over a telecommunications network without the knowledge of the person making or receiving the communication"

3.4.5. Interception of communications, save by authorized persons is illegal and attracts criminal punishment and a fine of $500,000.00 and or sentence of up to seven years imprisonment;[40]

3.4.6. The intentional possession, sale, purchases, or manufacture of a device or any component thereof, whose design renders it primarily useful for unauthorised interception of private communications is illegal and attracts criminal sanction of a fine in the sum of $250,000.00 and or imprisonment of up to five years;[41]

3.4.7. The Act like the Zimbabwean law has a class of authorized persons who can effect lawful interception | surveillance of communication;[42]

3.4.8. In Trinidad and Tobago the revenue authority is not part of the group of authorized persons;

3.4.9. Unlike in Zimbabwe, but like in South Africa the interception is authorized upon written and, in urgent cases, oral application to a Judge of the High Court upon reasonable cause being shown;[43]

3.4.10. Interception warrants are valid for three months and may be extended upon application to a Judge of the High Court;[44]

3.4.11. Telecommunications service providers have a duty to assist in the execution and enforcement of interception | surveillance warrants failing which they face summary conviction and a fine of $1,000,000.00; [45]

3.4.12. Intercepted communications which do not aid the intended purpose must be destroyed immediately after it becomes apparent that they are useless;[46]

3.4.13. Intercepted communications which would have served their purposes must be destroyed soon after serving their purpose;[47]

3.4.14. Failure to to destroy any record of information as required is an offence and attracts a fine of five hundred thousand dollars and imprisonment for seven years;[48]

3.5. **Interception of Communications Act, 1985 of the United Kingdom**

3.5.1. The Interception of Communications Act 1985 (1985 c. 56) was an Act of Parliament in the United Kingdom. It came into operation as of 10 April 1986;

3.5.2. The Act created the offence of unlawfully intercepting communications sent by post or by a "public telecommunications system"; those guilty were liable, on conviction, to a fine or up to two years imprisonment. It provided for a system of warrants to permit legal interception, and laid down cases where interception could be done lawfully, stating that having reasonable grounds to believe that the other party consented to interception was a defence;

3.5.3. The Act also established a complaints tribunal (which in 2000 was subsumed into the Investigatory Powers Tribunal), and created the post of Interception of Communications Commissioner to review the workings of the Act. It amended parts of the Telecommunications Act 1984.

3.5.4. This Act has since been repealed by schedule 1 of the Regulation of Investigatory Powers Act 2000.

3.6. **The Interception of Communications and Surveillance Ordinance Chapter 589 of Hong Kong**

3.6.1. The Ordinance provides a statutory regime for the authorisation and regulation of interception of communications and covert surveillance conducted by law enforcement agencies to prevent or detect serious crime and protect public security;

3.6.2. The Commissioner on Interception of Communications and Surveillance is an independent oversight authority, appointed by the Chief Executive on the recommendation of the Chief Justice;

3.6.3. The Code of Practice issued by the Secretary for Security pursuant to section 63 of the Ordinance provides practical guidance to officers of the law enforcement agencies in respect of matters provided for in the Ordinance.[49]

4. **Analysis and Recommendations**

4.1. The word **"surveillance"** is not used in the Interception of Communications Act of Zimbabwe but it is submitted that the word **"interception"** means the same as surveillance because in terms of Section 2 of the Act **"intercept"**, in relation to any communication which is sent—(a) by means of a telecommunication system or radiocommunication system, **means to listen to, record, or copy, whether in whole or in part; (b) by post, means to read or copy the contents, whether in whole or part;**

4.2. **"surveillance"** also takes the form of physical observation of people and their activities by state security officials or even other private persons and organisations. It is not provided for by the Zimbabwean laws but is known to happen and must be read into the larger body of law that permits the invasion of privacy;

4.3. **Test case requests for transparency reports**

4.3.1. Whilst the Act provides for the annual reporting to the Attorney General, said reports are as far as public documents go, unavailable;

4.3.2. It is recommended here that a request be made to the Minister, copied to the Attorney General, for the reports of the last eleven years since the Act became operational;

4.3.3. The requests ought to be made in terms of the Access to Information and Protection of Privacy Act with a view to finding out how many warrants have been issued, at whose instance and against who;

4.3.4. In the event of a refusal or other negative outcome, the request become a legal basis for instituting a test case to assert the right to access to information and also to have declared as *ultra vires* the Constitution some of the offending provisions of the law as was done by the South African High Court

4.4. **From outright interception to regulation of interception**

4.4.1. The tone and approach of the Zimbabwean legal framework is one of outright interception;

4.4.2. Whilst it is accepted that the world over interception and surveillance are a necessary evil, the rest of the world has moved on from mere interception to the regulation of the interceptions;

4.4.3. The regulation of the interceptions is a necessary safeguard that is also a best practice the world over;

4.4.4. In this regard the Interception of Communications Act may borrow heavily from the South African Regulation of Interception of Communications Act as well as the law of Trinidad and Tobago;

4.4.5. Notable regulation of interception provisions are the use of judges as opposed to public officials of the Executive arm of government;

4.4.6. In aiding the regulation of interception of communications, it may also be advisable to incorporate an independent monitoring authority as is the case in the United Kingdom and Hong Kong;

4.5. **<u>Authority to intercept communications</u>**

4.5.1. The vesting of the power to authorize the interception of communications in the Minister responsible for the administration of the Act is both undesirable and problematic;

4.5.2. It is undesirable because it flies in the face of the constitutional doctrine of separation of powers;

4.5.3. It is problematic because it creates a situation where the law enforcement agents, part of the executive arm of government, apply to their superior within the executive branch to carry out an executive assignment;

4.5.4. Judicial oversight regarding the constitutionality and other legality of the warrant is completely missing as the executive is not charged with the interpretation of legal rights relative to executive administrative conduct;

4.5.5. The right to the protection of the law, here read in part to mean the right to privacy, is completely negated by this arrangement and is only left to the tail end of a possible appeal to the Administrative Court of Zimbabwe way after damage has already been done;

4.5.6. The ideal situation is one where the authority to intercept is applied to and adjudicated upon by a judicial officer in the first instance;

4.5.7. In the Republic of South Africa, where the relevant Act provides for the appointment of a 'designated judge' by the Minister for purposes of adjudicating applications for interception warrants and or directives, the High Court has recently ruled that even the 'designated judge' appointed as he or she is by a minister is a violation of the Constitution and a proposal has been

made that such ministerial appointment be based on a list of nominees submitted by the Judicial Service Commission;

4.5.8. It is submitted that the right to a fair trial in the determination of the extent of one's civil and other legal obligations is the province of judicial authority as opposed to the executive;

4.5.9. In the Zimbabwean constitutional order, all judicial appointments are the province of the Judicial Service Commission, based on nominations from the public that are shortlisted by the Parliamentary Committee on Standing Rules and Orders in terms of Sections 180 (1) and (2);

4.5.10. Clearly therefore the norm in surveillance policy and legal frameworks is still to defer to judicial authority the granting or withholding of permission to intercept communications or otherwise lawfully invade privacy and it is respectfully submitted that Zimbabwe should be guided accordingly if the interception and or surveillance model is to guarantee sufficient safeguards and inspire public confidence;

4.6. <u>Reports and opinion of Attorney General should be publicized;</u>

4.6.1. Reports of the Minister should follow clear guidelines regarding matters to be reported on;

4.6.2. The Trinidad and Tobago Act is instructive in this regard and outlines the relevant items the Minister has to report on as follows:

"24. (1) The Minister shall, within three months, after the end of each year, in relation to the operation of the Act in the immediately preceding year, prepare a report relating to– (a) the number of warrants applied for to intercept communications; (b) the number of warrants granted by the Court; (c) the number of warrants applied for and granted under section 11; (d) the average period for which warrants were given; (e) the number of warrants refused or revoked by the Court; (f) the number of applications made for renewals; (g) the number and nature of interceptions made pursuant to the warrants granted; (h) the offences in respect of which warrants were granted, specifying the number of warrants given in respect of each of those offences; (i) the numbers of persons arrested whose identity became known to an authorised officer as a result of an

interception under a warrant; (j) the number of criminal proceedings commenced by the State in which private communications obtained by interception under a warrant were adduced in evidence and the number of those proceedings that resulted in a conviction; (k) the number of criminal investigations in which information obtained as a result of the interception of a private communication under a warrant was used although the private communication was not adduced in evidence in criminal proceedings commenced by the State as a result of the investigations; (l) the number of prosecutions commenced against persons under sections 6, 7, 8, 17, 19 and 21 and the outcome of those prosecutions; (m) a general assessment of the importance of interception of private communications for the investigation, detection, prevention and prosecution of offences in the State; and (n) any other matter he considers necessary. (2) The Minister shall cause a copy of the report prepared by him under subsection (1) to be laid before both Houses of Parliament within one month after its completion."

4.7. <u>Rights of interception|surveillance subjects|targets;</u>

4.7.1. There is no notice to a suspect before a warrant for the interception of their communication is applied for;

4.7.2. Warrants, and information intercepted may thus be acquired and only come to the attention of the owner at the point of arrest and or prosecution;

4.7.3. The law should make provision for a substantive right for persons and organisations to request service providers periodically to report to them the number of requests made in respect of their communications;

4.7.4. In the alternative, and in the same way service providers routinely advise on matters such as data consumption, call time etc, they should have a substantive duty to service users to furnish them with periodic reports made for warrants of interception by state security agents;

4.7.5. The absence of notice to the data subjects is not only a unilateral violation of privacy but is likewise a violation of the right to a free and fair trial;

4.7.6. As observed by Sutherland J in the ***Amabhungane Centre for Investigative Journalism NPC*** case at page 17ff

"[41]… pre-interception notice is self-evidently problematic. The idea is vulnerable to a cogent argument that to do so defeats the very purpose of the exercise. Thus, the focus of the application is on a post-surveillance-notice.

[42] This is no novel concern. In *Klass v Germany* ECHR [1978] 5029|71, the European court of Human Rights recognized the unhappy need for surveillance but nevertheless observed that one cannot undermine democracy on the grounds of defending it. It was held at [50] that:

"The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse."

[43] In broad terms, once it is assumed that secret surveillance is capable of justification, the controversial terrain is the risk of abuse, whether by zealous or corrupt official. Such a risk is not academic in South Africa. The whole safeguards model built into the statute must be examined and the presence or absence of a right to notice means, logically that the subjects of surveillance who have wrongfully had their privacy violated have no opportunity to initiate steps in a court to seek relief in respect of the abuse. Thus, the right to access to the courts as contemplated in Section 34[50] is indeed compromised… the right of notice is critically instrumental in securing a Section 34 right. Afterall, there can be no right without a remedy… the norm[51] is that unless reasons exist not to give notice, notice will be given. An independent authority makes that judgment call… In the jurisprudence of the European Court of Human Rights, a post-surveillance notice is an essential ingredient of a surveillance model that complies with Article 8 of the European Convention on Human Rights which guarantees privacy"

4.7.7. It is notable that efforts are presently underway to enact an Independent Complaints Commission in terms of a proposed Independent Complaints Commission Bill whose stated function will be "…the provision of an effective and independent mechanism for receiving and investigating complaints from members of the public against misconduct by members of the security services. Also included in the objects is the making of recommendations for disciplinary action to be taken against offending members, securing the grant of appropriate remedies to injured parties and the co-operation of the security services,

enhancing accountability and transparency by security services when discharging their functions."[52]

4.7.8. Hopefully this mechanism will likewise aid and supplement remedies for victims of unlawful or otherwise wrongful interceptions and or surveillance. As and when it becomes law.

4.11. Protection from private interception|surveillance devices

4.11.1. Whilst the Zimbabwe Act criminalises the unauthorized interception|surveillance of communications, it appears to ignore the prevalence of high level gadgets with such capacity that may be in the hands of private citizens;

4.11.2. It is imperative that, if privacy of persons is to be protected to the maximum, the law not only punishes unlawful interception|surveillance but also sanction the possession, manufacture, sale or other distribution of apparatus with such capacity;

4.12. Protection of journalists' sources

4.12.1. "61. (2) Every person is entitled to freedom of the media, which freedom includes protection of the confidentiality of journalists' sources of information… (5) Freedom of expression and freedom of the media exclude (a) incitement to violence; (b) advocacy of hatred or hate speech; (c) malicious injury to a person's reputation or dignity; or (d) malicious or unwarranted breach of a person's right to privacy."

4.12.2. "Media practitioners shall not be required to reveal confidential sources of information or to disclose other material held for journalistic purposes except in accordance with the following principles:

¬ the identity of the source is necessary for the investigation or prosecution of a serious crime, or the defence of a person accused of a criminal offence;

¬ the information or similar information leading to the same result cannot be obtained elsewhere;

¬ the public interest in disclosure outweighs the harm to freedom of expression; and

¬ disclosure has been ordered by a court, after a full hearing."[53]

4.12.3. In their current form, the legal provisions technically empower authorized officials to direct a journalist to disclose information about a source of information used in the course of the professional duties contrary to the constitutional **protection of the confidentiality of journalists' sources of information;[54]**

4.12.4. A journalist's communications with a source of information may likewise be intercepted under the guise of detection and or investigation of crime;

5. Conclusion

5.1. The current legal and policy framework is for the surveillance and interception of communications of citizens in Zimbabwe is wide open to legal challenge on the authority of the predecessor to the Constitutional Court of Zimbabwe in the case of ***Law Society of Zimbabwe v Minister of Transport & Anor.*** **SC – 59 – 03;**

5.2. The very persuasive judgment of the High Court of South Africa in ***Amabhungane Centre for Investigative Journalism NPC & Anor. V Minister of Justice and Correctional Services and 10 Ors*** **(as yet unreported judgement of the Gauteng Local Division per Sutherland J and handed down on 16th September 2019)** is likewise further basis for legal challenge;

5.3 It is now settled practice the world over that surveillance and interception of private communications are a necessary evil in the interests of public safety, public order, economic and other security interests;

5.4 What remains in need of further attention are the necessary safeguards to which citizens as data subjects can rely on for their protection as the lawful invasions of privacy are ongoing;

5.5 In Zimbabwe, the protection is at the tail end of the interception process i.e. to the Administrative Court but only after extensive damage may already have been done.

Endnotes

---

[1] For and on behalf of MISA – Zimbabwe, Tafadzwa Ralph Mugabe, LLBS (Hons) University of Zimbabwe, LLM (*cum laude)* University of Notre Dame, IP & ICT Counsel at Tafadzwa Ralph Mugabe | Legal Counsel 50 Lomagundi Road, Emerald Hill Harare trmugabe@trm.co.zw, www.trm.co.zw, +263775554408, +263242332613, +263242332614

[2] Section 57 of the Constitution of Zimbabwe, 2013

[3] Section 86 (1) of the Constitution *supra*

[4] Section 86 (2)

[5] Section 87 of the Constitution *supra*

[6] Published and put into operation on 15th March 2002 (General Notice 116/2002)

[7] Preamble to Access to Information and Protection of Privacy Act [*Chapter 10:27*]

[8] Section 2 of the Access to Information and Protection of Privacy Act

[9] Section 29 of the Access to Information and Protection of Privacy Act

[10] Section 30 (1) paragraphs (a) and (b) of the Access to Information and Protection of Privacy Act

[11] Section 30 (2) and (3) paragraphs (a) and (b) of the Access to Information and Protection of Privacy Act

[12] Section 33 of the Access to Information and Protection of Privacy Act

[13] Section 36 (a) and (b) of the Access to Information and Protection of Privacy Act

[14] Section 37 (a) and (b) of the Access to Information and Protection of Privacy Act

[15] See the reported cases of *S v Chikanga* SC- 93 -04; *S v Matinyenya* HH – 108 – 16; *S v Stanley* HH – 97 - 10; *S v Thomas & Ors* HB – 53 - 11; *Sv Madunga & Anor* HMA – 33 - 18; *S v Tsvangirai* HH – 169 - 04

[16] Sections 47 to 64 of the Criminal Procedure and evidence Act [*Chapter 9:07*]

[17] See Section 12 of the Civil Evidence Act as read with Section 62 (1) of the Constitution and the Access to Information and Protection of Privacy Act [soon to be repealed]

[18] Section 3 of the Act

[19] Section 8 of the Act

[20] THIRD SCHEDULE (Sections 32, 116 117(6) and 123)

Offences in Respect of Which power to admit Persons to Bail is Excluded or Qualified

Part I

1. Murder, where¾(a) it was planned or premeditated; or (b) the victim was¾
   (i) a law enforcement officer or public prosecutor performing his or her functions as such, whether on duty or not, or a law enforcement officer or public prosecutor who was killed by virtue of his or her holding such a position; or (ii) a person who has given or was likely to give material evidence with reference to any offence referred to in the First Schedule; or (c) the death of the victim was caused by the accused in committing or attempting to commit or after having committed or having attempted to commit one of the following offences¾ (i) rape; or (ii) aggravated indecent assault; or (iii) robbery with aggravating circumstances; or (d) the offence was committed by a person, group of persons or syndicate acting in the execution or furtherance of a common purpose or conspiracy.
2. Rape or aggravated indecent assault¾
   (a) when committed¾(i) in circumstances where the victim was raped or indecently assaulted more than once, whether by the accused or by any co-perpetrator or accomplice; or (ii) by

more than one person, where such persons acted in the execution or furtherance of a common purpose or conspiracy; or (iii) by a person who is charged with having committed two or more offences of rape or aggravated indecent assault; or (iv) by a person who knew that he or she had the acquired immune deficiency syndrome or the human immunodeficiency virus; or (b) where the victim¾ (i) is a girl or boy under the age of 16 years; or (ii) is a physically disabled woman who, due to her physical disability, is rendered particularly vulnerable; (iii) is mentally disordered or intellectually handicapped, as defined in section 2 of the Mental Health Act [*Chapter 15:12*] (No. 15 of 1996); (c) involving the infliction of grievous bodily harm.

3. Robbery, involving¾ (a) the use by the accused or any co-perpetrators or participants of a firearm; or (b) the infliction of grievous bodily harm by the accused or any co-perpetrators or participants; or (c) the taking of a motor vehicle as defined in section 2 of the Road Traffic Act [*Chapter 13:11*].

4. Indecent assault of a child under the age of 16 years, involving the infliction of grievous bodily harm.

5. Kidnapping or unlawful detention involving the infliction of grievous bodily harm.

6. Contravening section 20, 21, 22, 23, 24, 25, 26, 27 or 29 of the Criminal Law Code.

7. Contravening section 128 of the Parks and Wild Life Act [*Chapter 20:14*].

[Paragraph as substituted by s. 4 of Act No. 5 of 2011]

8. An offence referred to in Part II¾ (a) where the accused has previously been convicted of an offence referred to in that Part or this Part; or (b) which was allegedly committed whilst he or she was released on bail in respect of an offence referred to in that Part or this Part.

[Paragraph as inserted by s. 4 of Act No. 5 of 2011]

Part II

1. Treason.

2. Murder otherwise than in the circumstances referred to in paragraph 1 of Part I.

3. Attempted murder involving the infliction of grievous bodily harm.

4. Malicious damage to property involving arson.

5. Theft of a motor vehicle as defined in section 2 of the Road Traffic Act [*Chapter 13:11*].

6. Any offence relating to the dealing in or smuggling of ammunition, firearms, explosives or armaments, or the possession of an automatic or semi-automatic firearm, explosives or armaments.

7. A conspiracy, incitement or attempt to commit any offence referred to in paragraph 4, 5 or 6.

8. Any offence where the Prosecutor-General has notified a magistrate of his intention to indict the person concerned in terms of section 66.

[Paragraph amended by s. 33 of Act No. 5 of 2014 with effect from 2.1.2015]

[Schedule as substituted by s. 27 of Act No. 9 of 2006 and amended by s. 4 of Act No. 5 of 2011]

[21] NINTH SCHEDULE (Sections 25 (1) (a) and 32)

Offences involving Corruption, Organised Crime or Harm to the National Economy

1. Any offence referred to in Chapter IX ("Bribery and Corruption") of the Criminal Law Code.

2. Contravening section 63 ("Money-laundering") of the Serious Offences (Confiscation of Profits) Act [*Chapter 9:17*].

3. The sale, removal or disposal outside Zimbabwe of any controlled product in contravention of the Grain Marketing Act [*Chapter 18:14*].

4. Any offence under any enactment relating to the unlawful possession of, or dealing in, precious metals or precious stones.

5. Any offence referred to in Chapter VII ("Crimes Involving Dangerous Drugs") of the Criminal Law Code, other than unlawful possession or use of dangerous drugs where the dangerous drug in question is cannabis.

6. Fraud or forgery¾ (a) involving prejudice or potential prejudice to the State, except where the magnitude of the prejudice or potential prejudice is less than such amount as the Minister may prescribe by notice in a statutory instrument; or (b) committed by a person, group of persons, syndicate or enterprise acting in execution or furtherance of a common purpose or conspiracy; or (c) where the magnitude of the prejudice or potential prejudice to any person is more than such amount as the Minister may prescribe by notice in a statutory instrument.

7. Contravening section 42 ("Offences relating to banknotes") of the Reserve Bank Act [*Chapter 22:15*] or committing any offence relating to the coinage.

8. Contravening subparagraph (i) of paragraph (a) of subsection (1) of section 5 of the Exchange Control Act [*Chapter 22:05*] as read with¾ (a) subsection (1) of section 4 of the Exchange Control Regulations, 1996, published in Statutory Instrument 109 of 1996, (in this paragraph and paragraph 8 called "the Exchange Control Regulations"), by dealing in any foreign currency in contravention of paragraph (a) or (b) of that section of the Regulations without the permission of an exchange control authority; (b) subsection (1) of section 10 of the Exchange Control Regulations, by unlawfully making any payment, placing any money or accepting any payment in contravention of paragraph (a), (b), (c) or (d) of that section of the Regulations; (c) paragraph (a) or (b) of subsection (1) of section 11 of the Exchange Control Regulations, by unlawfully making any payment outside Zimbabwe or incurring an obligation to make any payment outside Zimbabwe; (d) paragraph (b). (e) or (f) of subsection (1) of section 20 of the Exchange Control Regulations, by unlawfully exporting any foreign currency, gold, silver or platinum, or any article manufactured from or containing gold, silver or platinum, or any precious or semiprecious stone or pearl from Zimbabwe; (e) subsection (2) of section 21 of the Exchange Control Regulations, by unlawfully exporting any goods from Zimbabwe in contravention of that provision of the Regulations.

[22] Section 5 (1) of the Act

[23] Section 4 of the Act

[24] Sections 10 and 12 of the Act. See for example such technology on offer called utimaco© in the following terms: **"**LIMS - a Carrier-grade LI Solution**.** The Utimaco Lawful Interception Management System (LIMS) is a state-of-the-art monitoring solution for fixed and mobile networks. It helps telecom operators and Internet service providers fulfill their legal obligation to intercept calls and data while maintaining maximum privacy protection. Utimaco LIMS enables target-based monitoring of public communications services including telephone calls, mobile data and Internet-based services such as e-mail, Voice-over-IP, instant messaging and others. The system acts as a bridge or mediator between the service provider's network and the law enforcement's monitoring centers. Strong security provisions prevent unauthorized access, secure all private user data and facilitate security audits by comprehensive logging." https://lims.utimaco.com/products/lawful-interception-management-system/?gclid=CjwKCAjwnrjrBRAMEiwAXsCc454QcxKs_mnFeSix4Alb9l2UceEhVjFTGZmmSQLtxWi48sYzapV0axoC7CIQAvD_BwE accessed 4th September 2019

[25] See Section 11 of the Act as read with the Criminal Law Codification and Reform Act (Standard Scale of Fines) Notice, 2019 Statutory instrument 209 of 2019 dated 23rd September 2019

[26] See Sections 14 and 15 of the Act as read with the (Standard Scale of Fines) Notice, 2019 above

[27] See Sections 16 (1) and (2) of the Act

[28] See Section 16 (3) of the Act

[29] See Section 17 of the Act

[30] See Section 18 of the Act

[31] See Section 19 of the Act

[32] See Section 20 of the Act

[33] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance Accessed 4th September 2019

[34] [53] The applicant seeks the following declaration:

"It is declared that: (a) RICA, including sections 16(7), 17(6), 18(3)(a), 19(6), 20(6), 21(6) and 22(7) thereof, is inconsistent with the Constitution and accordingly invalid to the extent that it fails to prescribe procedure for notifying the subject of the interception; (b) The declaration of invalidity is suspended for two years to allow Parliament to cure the defect; and (c) Pending the enactment of legislation to cure the defect, RICA shall be deemed to read to include the following additional sections 16(11) and (12): (11) The applicant that obtained the interception direction shall, within 90 days of its expiry, notify in writing the person who was the subject of the interception and shall certify to the designated judge that the person has been so notified. (12) The designated judge may in exceptional circumstances and on written application made before the expiry of the 90 day period referred to in sub-section (11), direct that the obligation referred to in sub-section (11) is postponed for a further appropriate period, which period shall not exceed 180 days."' [54] Immediate interim relief is self-evidently appropriate. Save with one qualification, in my view, the proposed interim text is appropriate. The cruel fact must be recognised that a deferral of notice in *de facto* perpetuity is sometimes legitimate. That is, of course, an extreme position. For that reason I would add a proposed (13). That text would go hand in hand with a tail to proposed subsection (12) to read:" ....exceed 180 days at a time." The text of (13) would read:"In the event that orders of deferral of notification, in total, amount to three years after surveillance has ended, the application for any further deferral shall be placed before a panel of three designated judges for consideration henceforth, and such panel, as constituted from time to time, by a majority if necessary, shall decide on whether annual deferrals from that moment forward should be ordered." Per Sunderland J in ***Amabhungane Centre for Investigative Journalism NPC & Anor. V Minister of Justice and Correctional Services and 10 Ors*** (as yet unreported judgement of the Gauteng Local Division per Sutherland J and handed down on 16th September 2019)

[35] At paragraph [71] of the judgment in ***Amabhungane Centre for Investigative Journalism NPC & Anor*** above

[36] At paragraph [82] of the judgment in ***Amabhungane Centre for Investigative Journalism NPC & Anor*** above

[37] At paragraph [108] of the judgment in ***Amabhungane Centre for Investigative Journalism NPC & Anor*** above

[38] See Preamble to Interception of Communications Act [*Chapter 15:08*] which states as follows:

"WHEREAS it is enacted by section 13(1) of the Constitution that an Act of Parliament to which that section applies **may expressly declare that it shall have effect even though inconsistent with sections 4 and 5 of the Constitution** and, if any Act does so declare, it shall have effect accordingly: And whereas it is provided in section 13(2) of the Constitution that an Act of Parliament to which that section applies is one the Bill for which has been passed by both Houses of Parliament and at the final vote thereon in each House has been supported by the votes of not less than three-fifths of all the members of that House: And whereas it is necessary and expedient that the provisions of this Act shall have effect even though inconsistent with sections 4 and 5 of the Constitution:

2. This Act shall have effect even though inconsistent with sections 4 and 5 of the Constitution."

[39] See Short Title to Interception of Communications Act [*Chapter 15:08*]

[40] See Section 6 (1) of Interception of Communications Act [*Chapter 15:08*]

[41] See Section 7 (1) of Interception of Communications Act [*Chapter 15:08*]

[42] Chief of Defence Staff, the Commissioner of Police or the Director of the Strategic Services Agency;

[43] See Section 8 as read with Section 11 (1) of Interception of Communications Act [*Chapter 15:08*]

[44] See Section 10 of Interception of Communications Act [*Chapter 15:08*]

[45] See Section 13 of Interception of Communications Act [*Chapter 15:08*]

[46] See Section 20 (1) of Interception of Communications Act [*Chapter 15:08*]

[47] See Section 20 (2) of Interception of Communications Act [*Chapter 15:08*]

[48] See Section 20 (7) of Interception of Communications Act [*Chapter 15:08*]

[49] Available at https://www.sb.gov.hk/eng/special/sciocs/2016/ICSO%20CoP%20-%20June%202016%20(E).pdf

[50] Section 69 of the Constitution of Zimbabwe, 2013

[51] See the references to Canada, Germany, Japan and the United States of America which all variously provide for the post – surveillance notices as well as the interim relief granted in the ***Amabhungane*** judgment

[52] Draft Independent Complaints Commission Bill, 2019 available at http://www.ca-lr.org/download/independent-complaints-commission-bill/

Accessed 2nd October 2019

[53] Article XV of the *Declaration on principles of Freedom of Expression in Africa of 2002*

[54] Constitution of Zimbabwe, 2013