Analysis of the Interception of Communication Bill 2006: Interception and deception!

Jacob Mapfume for Media Institute of Southern Africa-Zimbabwe Chapter
April 21, 2006

Background

Zimbabweans have witnessed the promulgation[1] of a number of, repressive laws, which have contributed to the shrinking of the democratic space and the operating environment of human rights defenders and activists. The introduction of the Interception of Communications Bill (hereinafter the Bill) adds to the number of laws, which have attacked the enjoyment, and furtherance of human rights in Zimbabwe, in particular freedom of expression and right to receive and impart information among other rights. The following analysis gives simplified understanding of the implications of passing such a law in its currents state and requirements and obligations of the government of Zimbabwe in terms of its constitutional, international and regional human rights law obligation.

SUMMARY OF THE BILL AND INTRODUCTORY OBSERVATIONS

Part 1 & 2

The object of the Bill as stated in the introductory memorandum and the long title, is to give effect to Interception of Communications Monitoring Center, shall have the mandate to implement the provisions of the Bill, thus to intercept communications in the course of their transmission through either telecommunications, postal emails and any other related service.

Part 3

The Bill specifies the persons who shall have authority to make applications for interception of communication. Certain officers who are directly under the Office of the President or Executive are empowered to make applications for authorized interceptions of communications; these individuals include the Chief of Defense Intelligence, the Director-General of the President's Department of the National Security, The Commissioner of Zimbabwe Republic Police and the Commissioner General of the Zimbabwe Revenue Authority.

The above persons who occupy critical offices in terms of economic and political security of the state can make representations to the Minister (of Transport and Communications or any other Minister to whom the functions can be assigned by the President) for conducting of interceptions. A warrant of interception is granted on reasonable grounds or belief that a serious offence has been or is being or will be committed or that there is a threat to safety or "national security" of the country or the information might be of compelling national economic interests of the country. National security of Zimbabwe includes matters relating to the existence, independence and safety of the state. The warrant lasts for 3 months and can be renewed every month until such a time that the intended interception has been undertaken. The powers granted to the security officers in this Bill are subject to judicial scrutiny, however there are high probabilities abuse of power by targeting organizations and individuals. This Bill will obviously target legitimate political activists and organizations that have been targeted in the past by state institutions and laws[2]. Such provisions are in clear violation of the right to

---

[1] Public Order and Security Act, which has seen hundreds of human rights defenders being arrested, detained and prosecuted since enactment in….., the Miscellaneous Offences Act remnant of some of the laws passed in the colonial era, Access to Information and Protection of Privacy Act, the Zimbabwe Electoral Commission Act, Electoral Act, Constitutional Amendment 17, Non Governmental Organizations Bill

[2] Remarks of Minister Patrick Chinamasa on the passing of Constitutional Amendment No 17 IRIN website

freedom of expression and privacy as stipulated in Constitution of Zimbabwe and various supra national human rights instruments which Zimbabwe has ratified[3].

The Bill states that information, which has been intercepted, shall not be disclosed to any other person except, where the information is required in any proceedings in any court of law.

Part 4

The Bill also provides for general prohibitions and exemptions from disclosure of any information that is obtained in the exercise of duty in terms of the Bill. The Bill allows only authorized persons that execute the interception of communication to disclose to extend the proper performance of duties. It authorizes the destruction as soon as possible the information that shall be intercepted.

The Bill states that the authorized persons can apply for the detention order to detain any postal article which they suspect contains anything in respect of which an offence or attempted offence is being committed. The Bill does not specify the nature of offences or grounds that are deemed a threat to national security, this adds to a plethora of laws that have been enacted under the guise of being "a state under siege". The ambiguity will give them, ground to intercept the communications on unreasonable grounds, which are not reasonably justifiable in a democracy. The grounds under which an application for interception can be made are open to abuse thus a broad array of offences, which leaves many members of civil society at arms way, and thus run the risk of having their communications intercepted, recorded and used in courts of law against them.[4]

It is important for Parliament and the citizens that are going to be subjected to this Bill to conceptualize the right to freedom of expression and privacy under the various provisions of the International Covenant on Civil and Political Rights, the African Charter on Human and Peoples Rights and the Universal Declaration of Human Rights. While factoring and debating the substantive and procedural as well as the protectionist attributes of the Bill it should do so in light of minimum standards that are universally acceptable and as set out by international human rights declarations.

The Bill in context of Zimbabwe's International obligations

Freedom of expression and right to privacy as enshrined in various international instruments such as the ICCPR and the UDHR have become universally accepted. While Zimbabwe might argue non-domestication of various international and regional human rights instruments, the obligation to attain the rights as provided in these instruments is the founding spirit of such. Countries and state parties to these instruments are mandated to take positive steps towards the realization of the rights, these measures cane either be legal or administrative measures. It is therefore important to emphasis that while drafting and debating this Bill it is essential for Parliament to note that the full respect of freedom of expression and information by States and non-State actors is an essential precondition for the building of a free and independent democratic society.

The promulgation of such legislation will no doubt cast aspersions and confirm that Zimbabwe is far from being a democratic state and this kind of legislation is no doubt, intended to undermine section 20 of the Zimbabwe Lancaster Constitution. The Executive and Legislative have made it a practice to pass laws in particular constitutional amendments, which repeal

---

[3] International Covenant on Civil and Political Rights Article…. May 1990, African Charter on Human and Peoples Rights, Article…. June 1987 , Universal Declaration of Human Rights, SADC Protocols…

[4] Customer defined as any person, body or organization which has entered into a contract with the service provider for the provision of a telecommunications service to that person, body or organization in terms of the Bill.

decisions of the Supreme Court[5]. The coming into force of this Bill will mean a legislative repealing or reversal of a judicial decision as the Supreme Court ruled in 2004 on similar provisions of the Postal and Telecommunications Act (PTC Act). The Supreme Court sitting as a constitutional bench declared unconstitutional Sections 98 and 103 of the PTC Act for the reason that it violated Section 20 of the Constitution of Zimbabwe, which provides for freedom of expression, freedom to receive and impart ideas and freedom from interference with one's correspondence. The Supreme Court held that the presidential powers provided for therein, that is to intercept mail; telephone calls, e-mail and any other form of communication were unconstitutional. Until such a law has been gazetted Zimbabweans are legally protected from such machinations and the blatant attempts to give a semblance of legality to acts of intrusion by a government, which purports to uphold fundamental rights and freedoms[6].

Article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights is of fundamental importance to a human rights-based information and communication society. This is based on the fact that everyone has the right to freedom of opinion and expression and the right to seek, receive and impart information and ideas through any media and regardless of frontiers, but also because it implies free flow of information and free circulation of ideas, press freedom. Therefore, it is important for parliament to consider various articles and principles that are set out in the international instruments before they pass a law that clearly impounds the rights of its citizen thus violating the rights that have come to be recognized, respected and upheld internationally.

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Convenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech.[7] It has become one of the most important human rights issues of the modern age. The right to privacy although not stipulated in the Zimbabwean Constitution has come to be recognized internationally as a human right and thus Zimbabwe having ratified these international treaties is under obligation to respect these rights. These instruments enshrine privacy as a core human right or value that goes to the very heart of preserving human dignity and autonomy. Therefore, by setting up the Monitoring Center to intercept communications through enacting of a law that does not meet these standards, this law will be an out-right violation of the right to privacy, thus unprecedented possibilities for massive violations of the human rights, not only rights to privacy but expression and thus a continued regime of oppression.

The interception of such communications constitutes a breach of international human rights law, Articles ICCPR and Article of the African Charter on Human and Peoples Rights and therefore has to be justified in by being in accordance with the law, necessary in a democratic society, and in the interests of national security, public safety, or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. The Bill must provide for adequate measures to safeguard against the arbitrary use of the interception powers against citizens, it must also be clear and precise to give citizens circumstances in and conditions in which public officers are authorized to carry out interceptions.

In the several jurisdictions, the interception of all communications has been held to constitute a serious breach. In the European Court of Human Rights [8] the court has ruled on numerous

---

[5] This has been the case in decisions about outlawing of corporal punishment, Constitution of Zimbabwe Amendment (No. 13) Act, 1993, Constitution of Zimbabwe Amendment (No. 11) Act, 1990

[6] Law Society of Zimbabwe vs. the Minister of Information or President check the correct citation of the case

[7] Privacy and Human Rights: An International survey of privacy laws and practice, *http://www.gilc.org/privacy/survey/intro.html* viewed 23/03/06

[8] Kruslin v France (1990) 12 EHRR 547, Havig v France (1990) 12 EHRR 528 para 33 and 32 respectively

occasions “tapping and other forms of interception of telephone conversations constitute a serious interference with the private life and correspondence and must accordingly be based on a law that is particularly precise”.

Zimbabwe is one of the countries that are trying to enact laws that intercept communication under the pretext of national security yet other countries are trying to regulate the interception of communications through the enactment of constitutional provisions protecting the privacy of communications and laws and regulations to implement the constitutional requirements. Article 12 of the UDHR and Article 17 of the ICCPR states that

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks”. Therefore, in the process of enacting or threatening to enact this legislation is important to remind not only parliament but also the Ministry that originated this legislation that it does not meet the minimum international standards.

Although there are exceptions in the ICCPR on the right to privacy on the grounds of natural security, it’s important to point out that Zimbabwe over the last few years has made a habit to view organizations and institutions that point out human rights violations as institutions that are threatening national security. Therefore, this legislation will only worsen the situation of civic society organizations that are already on the hit-list of police and constantly intimidated with arbitrary detentions and arrest with no evidence or reasonable charge to detain them.

The Inter- American Commission just like the African commission have come up with basic principles on freedom of expression that need to be put into consideration when analyzing and debating this legislation.

The **Declaration of Principles on Freedom of Expression in Africa**[9]
Guarantees that Freedom of Expression includes the right to seek, receive and impart information and ideas. Either orally, in writing or in print, in the form of art, or through any other form of communication, including across frontiers, as a fundamental and inalienable human right and an indispensable component of democracy and states that everyone shall have an equal opportunity to exercise the right to freedom of expression and to access information without discrimination.

The Inter-American commission has gone further to draft the principles of freedom of expression and it is important to analyze these principles as a “democratic society”. The principles of freedom of expression, which are critical and are ignored by the Bill, are articles 1, 5, 7 and 8, which state that [10]

> 1. Freedom of expression in all its forms and manifestations is a fundamental and inalienable right of all individuals. Additionally, it is an indispensable requirement for the very existence of a democratic society.
>
> 5. Prior censorship, direct or indirect interference in or pressure exerted upon any expression, opinion or information transmitted through any means of oral, written, artistic, visual or electronic communication must be prohibited by law. Restrictions to the free circulation of ideas and opinions, as well as the arbitrary imposition of information and the imposition of obstacles to the free flow of information violate the right to freedom of expression.
>
> 7. Prior conditioning of expressions, such as truthfulness, timeliness or impartiality, is incompatible with the right to freedom of expression recognized in international

---

[9] African Commission on Human & Peoples' Rights, African Union Adopted by The African Commission on Human and Peoples' Rights, meeting at its 32nd Ordinary Session, in Banjul, The Gambia, from 17-23 October 2002

[10] Inter American Commission on Human Rights. Declaration principles on freedom of expression. http://www.cidh.org/DefaultE.htm

instruments.

8. Every social communicator has the right to keep his/her source of information, notes, personal and professional archives confidential.

These principles are basic requirements that a democratic state is expected to meet in the promotion of freedom of expression. It is of utmost importance that the debate and appraisal of clauses of the Bill must also take into account decisions of the courts which, in the past years, have been crucial in conceptualization of the scope and content of as well as exemptions to the constitutionally guaranteed right of freedom of expression which include, the following–

Analysis of the Substantive Parts and Clauses of the Bill

There are serious concerns that arise in regard to the compliance of this bill in its present form. The clauses in there current state necessitate serious reconsideration. It is vital that Zimbabwe adopts a progressive approach and reconsider the entire Bill. This section summarizes the various clauses and points out the implications of the provisions with reference to the international regional and human rights standards that have been set out.

Part 1 – Preliminary (clauses 1-2)

The definition/interpretation section (clause 2) needs to be systematic and embracing the terms and phrases used in the Bill. The definitions/interpretation should be put in context of the Bill's other provisions. There is need to constrict the definition of '**national security**". The definition of national security is so broad and not precise. National security has been defined as "matters relating to the existence, independence and safety of the state". The various international legal and regional instruments state that one can intercept communication if they believe that there is a threat to "national security". These very instruments demand that, to intercept communication on the foundation of national security the country has to be a **"democratic state"** and there is authentication of respect of the rule of law. It is therefore necessary to state that this bill's unsatisfactory definition of "national security" is, only intended to silence, limit and clampdown, further, on freedom of expression.

Part 2 – Preliminary (clauses 3-4)

Clause 3 This intends to control the interception of communication by unauthorized persons, which criminalizes the act of such persons found intercepting communication in violation of this Act to either imprisonment of five years or fine of level fourteen. However, this does not apply to persons who have been authorized by the Minister, or a person who is party to the communication or they have the consent of the person to whom the communication is sent.

Clause 4 Establishes the monitoring center which will be the sole facility, where all authorized interception shall be effected the center will be manned, controlled and operated by designated technical experts from the agency.

In this kind of situation, it is not logical to have the minister issue a warrant to intercept communications. It would be of great importance that such warrants are issued by an objective body in this case, the judiciary. It would be the most practical body that should authorize the issuing of a warrant to intercept, as the court will be required to evaluate the allegations and put them to the test of other laws before such a warrant is issued. Otherwise, there is a risk that the minister as a member of the Executive arm of government is biased and therefore will not be objective. It is important that before such a warrant is issued, the allegations made by the applicant be examined in a court of law to ensure that such allegations raised are genuine concerns to the national security.

Part 3 – Preliminary (clauses 5-14) application for lawful interception.

Clause 5 states that the categories of persons who can apply to intercept communications are persons who hold either political or Economic posts within the country.

> There is a need as earlier stated to remove such power that is granted to the Minister in this Bill since he is a prejudiced person. A judicial body would be the most appropriate institution to analyze the applications with the presence of the affected person so that they have an opportunity to defend themselves.

Clause 5 (3) a-e lays down the necessary information that an applicant has to provide before they make the application to intercept communication.

> These procedural issues need to be analyzed by a tribunal or judicial body especially in regard to evaluating the evidence brought forward by the applicant in regard to issuance of the warrant to intercept communication. Therefore, such applications need to be analyzed to ensure that all necessary investigative procedures have been administered and that they are unlikely to succeed. It is imperative that the courts of law put to test such allegations instead of the Minister of communication.

Clause 6 The minister shall issue the warrant to an applicant if they can affirm that a serious offence has been, or will be committed and that the information proves an actual threat to national security or national economic interests of the country or a threat to the countries interests in international relations or obligations.

> This clause is a major claw back on the right to privacy and correspondence of the private person. It has become tolerable under international and regional law that a country can intervene and intercept communications if there is a threat to the security of the country. However, various declarations have gone further to set standards in relation to the kind of government that can be sheltered under this exception. It has to be a democratic state that upholds the rule of law.
> Zimbabwe at this particular moment cannot be recognized as a democratic state. There have been unprecedented human rights violations, illegal detentions, enactment of repressive laws and clampdown on media freedoms. The citizens have witnessed a regime that does not respect or uphold the rule of law. Various jurisdictions have expanded the standards to state that in order to be “in accordance with the law” it is not sufficient for a measure to be based upon statue law. In the Kopp[11] case, the court held that additional requirements apply in terms of the quality of the law concerning accessibility to the person concerned and that person is able to foresee its consequences for him/her necessitating its compatible with the rule of law. The Court stated that the law in question had to be ‘compatible with the rule of law'. Concerning interception of communications by public authorities, they risk lack of public scrutiny; misuse of power and it is imperative that the domestic law must provide some protection to the individual against arbitrary interference. Thus, the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures.

Clause 6 (2) the clause states that in instances of urgency or exceptional circumstances an oral application may be made to the minister if the authorized person is of the opinion that it is not reasonable to make a written application.

> This exception is dangerous as the Minister can easily abuse the power given to him. It is important to state that the minister is a biased person in this situation she/he can easily forego the procedure laid out under the alleged reason that it is an urgent application and therefore use this clause to manipulate the situation. This section poses a great danger to Human Rights Defenders. Where their work will be

[11] (1999) 27 EHRR 91

intercepted under such un-procedural mechanisms that are intended to shut down the work of various human rights organizations. This clause is internationally unaccepted as the person, as earlier stipulated, will be unaware of what is happening and yet that evidence gathered can be used against him or her in the courts of law.

Clause 7 the warrant shall be valid for a period of three months and can be renewed for periods not exceeding one month. The warrant shall specify the name and address to which the interception shall take place or the facilities that shall be intercepted. It shall order the service provider to strictly comply with the technical requirements as may be required by the agency.

The warrant does not state the expiration period of the warrant after the one-month renewal. This gap could lead to abuse of power by the applicants since they can continue to monitor and intercept communication of a private person for an indefinite period.

Clause 8 The person shall disclose the contents of the whole or part of any communications, which has been intercepted in terms of the warrant except in as far as it may be necessary for the purpose for which the warrant was issued.

This clause leaves a lot of room for abuse of the person's right to privacy, as they are not informed about the interception.

Clause 9 states that evidence required by unlawful interception will not be admissible in criminal proceedings.
Kelly v Pickering and anor[12] stated the legal position

Clause 10 states that the various postal, or telecommunications systems should ensure that they are capable to support lawful interception, full interception at all material times. Which information shall be transmitted to the monitoring facility. The communication service providers are expected to provide access to all interception subjects operating temporarily or permanently within the communications systems. In instances where calls are diverted to other communications service providers or terminal equipment, the communication service are expected to have the capacity to implement a number of simultaneous interceptions to allow monitoring by more then one authorized person, also safeguard the identities of the monitoring agents, and ensure the confidentiality of the investigations. That the interceptions should be made in a manner that neither the interception target nor any other unauthorized persons is aware of any changes made to fulfil the interception order.

In other jurisdictions, it has been held that tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence.[13] Thus, it is necessary to have clear laws that allow a person to enjoy the minimum degree of protection required by the rule of law. This clause like the rest is a continued violation of the rights of an individual.

Clause 10 (2) This states that a communications service provider that fails to compile with clause shall be found guilty of an offence and liable to a fine not exceeding level twelve or imprisonment three years.

The criminalization of failure to comply is an outright violation of the right to privacy. The companies have the duty not to disclose information about their clients unless certified by the courts of law.

There is a violation of client service privilege in this instance. The service providers have a duty to keep their clients' information confidential. However, this bill intends to violate this duty.

---

[12] 1980(!) ZLR 44

[13] Kopp V Switzerland (199) 27 EHRR 91

It is therefore important to reiterate that the courts should be the institutions that issue the warrants and not the minister. It should also be there duty to examine the application made to intercept the communication.
This clause not only does it have financial implications on the various companies it continues to threaten the very existence of the right to privacy. The idea of criminalizing failure to comply with the set out rules is a clear violation of international and regional instruments.

Clause 11 states the duties of the telecommunication service provider and customer were they are expected to take the necessary details about their client and ensure that proper records of the client and whatever information that is brought to their attention.

Clause 12 states that if an authorized person believes that a key to the protected information is in possession of any person and that imposition of a disclosure requirement in respect of the protected information is necessary in the interests of national security. Where it is impracticable for the authorized person to obtain possession of the protected information in an intelligible form without giving notice under this section the authorized person may by notice to the person whom or he or she believes to have possession of the key, impose a disclosure requirement in respect of the protected information.

The notice shall be in writing and the person to whom the notice is given may use the key in his possession to provide access to information, and will be required disclose that information in an intelligible form. The person holding the security key shall be expected to disclose any information protected by a security key to an authorized person.

If the person to whom notice has been given is in possession of different keys, it shall not be necessary for the person to disclose other keys. However if a person to whom the notice has been given has been in possession of the keys but is no longer in possession of them he or she must disclose all such information as is in his or her possession to the authorized person.

- An authorized person will use this information only as specified by the notice or destroy the information if such information would not be use in criminal or civil cases.
- The person who fails to make the disclosure under this clause is guilty of an offence and is liable to a fine not exceeding twenty million or not exceeding five years or both fine and imprisonment.

In this situation the person runs the risk of self-incriminating themselves and thus a breach of the person's right to remain silent and which right has come to be internationally accepted under any questioning especially police questioning.

There are serious concerns about compromise of security concerning disclosure of keys to protected information. It also makes provision for failure to disclose and tipping off third parties that a notice has been given. In this case, disclosure is a rule and not an option by the person with the security key. This has a consequence of compromising the security of that person.

There is no provision that provides for supervision of the person when they are decrypting the information that is obtained from the person holding the security key. In the case of *Kruslin v huving* it is mentioned that there is need to state minimum standards to avoid abuse of power.

The bill criminalizes failure to disclosure if they hold the security key. However, it is extremely easy for the person to forget a password. In this case, if a person discloses they could be self-incriminating themselves.

Clause 13 this clause anticipates that telecommunication service should have the capability to intercepted and store the communication related information. The Minister will make a directive on how the telecommunications companies will affect the security and technical

requirements and how they can route the intercepted inform to the communication Monitoring Center which activity shall be done at the expense of the service providers.

This is a violation of the right to private property, which is internationally recognized and respected. This right ought to be respected and protected in human community life it's important to note that when the right to private property is not respected and not sufficiently protected, then there is something wrong with a community.

Clause 14 the minister shall prescribe the forms of assistance that will be rendered to the service providers and this will be concerning direct costs in respect of personal and administration, which are required for purposes of providing any forms of assistance

Part 4 – Preliminary (clauses 15-21) General prohibitions and exemptions.

Clause 15 prohibits disclosure and criminalizes such disclosure; the person found guilty will be sentenced to five years or fined ten million dollars. Authorized persons can disclose information to the extent that such disclosure is necessary.

Clause 16 the authorized persons however can disclose the intercepted information for the proper performance of his duties.

Clause 17 the authorized person shall destroy beyond retrievable proportions as soon as possible any intercepted product.

Clause 18 provides for detention of postal articles for purposes of examination and such an application can be made to the minister.

Clause 19 deals with examination of the detained postal articles, and states that if the article is found substantial then it can either be destroyed, or used for prosecution or and if found not substantial then it shall be delivered to the person to whom its addressed.

Clause 20 provides for appeals if a person is aggrieved, they can apply to the Minster within 14 days and if a person is aggrieved by the decision of the minister my appeal against it in the administrative court within one month after being notified of the decision that may confirm or set aside the decision.

Clause 21 provides for making of regulations by the minister.

> The minister in this clause has all the unrestricted power to make regulations as he deems fit, which may lead to serious abuse of power by the minister.

Rashweat Mukundu
MISA-Zimbabwe
Box HR 8113
Harare
Zimbabwe
Tel/fax 00 263 4 77 61 65, 746 838
Mobile 00 263 11 603 439
E mail director.misa@zimbaweb.net
Website: www.misazim.co.zw