INTERCEPTION OF COMMUNICATIONS BILL, 2006
(HB 4, 2006)

INTRODUCTION

The Interception of Communications Bill, 2006, was published in the Government *Gazette* on Friday 27 May, 2006. I have been asked to advise whether, if it is enacted into law, it will contravene the Declaration of Rights in the Constitution and, generally, what its effect is likely to be on human rights in Zimbabwe.

OUTLINE OF THE BILL

The aim of the Bill is to permit the Government to intercept and monitor communications[1] where it is considered necessary to do so in the national interest or to prevent serious offences. In furtherance of this aim, the Bill will establish a monitoring centre through which communications are to be intercepted and will require operators of postal and telecommunications services to provide the Government with whatever assistance may be needed to enable communications to be monitored.

The Bill starts with a general prohibition against the unauthorised interception[2] of communications transmitted by telephone or radio or through the post. No one, according to clause 3 of the Bill, will be allowed to listen to, read, record or copy such a communication unless he or she is a party to it (in the case of an electronic communication), or unless he or she does so with the permission of the sender or intended recipient of the communication, or unless the Minister of Transport and Communications has issued a warrant in terms of clause 6 of the Bill authorising its interception. Anyone who intentionally intercepts a communication in any other circumstances will be liable to imprisonment for up to five years.

This is a fairly encouraging start to the Bill, but it's downhill all the way from there.

Clause 4 of the Bill provides for the setting up of an entity called a "monitoring centre", a central monitoring apparatus which is to be "the sole facility through which authorised interceptions are effected." It will be manned and operated by technical experts designated by the "agency", which is defined as:

> "the government telecommunications agency comprising telecommunications experts which has been designated to operate the monitoring facility and which gives technical directions to service providers so as to ensure compliance with the provisions of this Act".

---

[1] The term "communication" is not defined in the Bill. Although clause 2(2) of the Bill states that definitions in the Postal and Telecommunications Act [*Chapter 12:05*] apply to words used in the Bill, the definition of "communication" in that Act applies only to telephonic and wireless communications, and it is clear from clause 3(1)(b) that in the Bill the word is intended to cover letters and other postal communications as well.

[2] "Intercept" is defined in clause 2(1) of the Bill as meaning to listen to, record or copy a communication sent by telephone or wireless, or to read or copy a communication sent by post. Reading of e-mails, therefore, does not seem to constitute "interception".

This is a remarkably opaque definition. There is no real explanation of what the "government telecommunication agency" is, or who is to designate it, or where the telecommunications experts who will comprise it are to come from. The phrase "monitoring facility" may be a mistaken reference to the monitoring centre, but it adds to the opacity. One fears that all this obscurity is a cloak to hide the fact that the monitoring centre will be operated by secret policemen from the President's Office.

Clauses 5 and 6 of the Bill empower the Minister of Transport and Communications to issue warrants for the interception of communications. The only people who will be able to apply for warrants are the Chief of Defence Intelligence, the Director-General of the organisation commonly known as the C.I.O., the Commissioner of Police and the Commissioner-General of the Zimbabwe Revenue Authority, and their nominees.[3] These people are collectively referred to in the Bill as "authorised persons". An authorised person who applies for a warrant will have to put his application in writing, setting out details of why he considers it necessary to intercept the communication concerned, though in cases of urgency oral applications will be permitted.[4] Understandably perhaps, there is no provision for notifying the person whose communications are to be intercepted and inviting him or her to make representations on the question of whether or not a warrant should be issued. Less understandably, there is also no provision for the service provider concerned to be notified.

On receipt of an application from an authorised person, the Minister will[5] issue an interception warrant if he has reasonable grounds for believing that:

- a serious offence has been, is being or will probably be committed;
- it is necessary to gather information concerning an actual threat to national security or a "compelling national economic interest";
- it is necessary to gather information concerning a "potential threat to public safety or national security"; or
- there is "a threat to the national interest involving the State's international relations or obligations".[6]

These are broad and vaguely-stated grounds indeed. The term "national security of Zimbabwe" is defined in clause 2(1) as including "matters relating to the existence, independence and safety of the State", but the grounds for issuing a warrant under clause 6 go further: they include the actual or probable commission of a serious offence[7]; an actual threat to a compelling national economic interest; a potential threat to public safety; and a threat to the State's international relations (whether the threat must be actual or potential is not stated). It should be noted that there is no statement in clause 6 that the Minister must be satisfied that interception of a particular communication will assist in the investigation, detection or prevention of a serious offence, or that it will help to avert a threat to the State's international relations; nor that he must be satisfied that intercepting a particular communication will form part of the infor

---

[3] Clause 5(1) & (2) of the Bill.

[4] See clauses 5(3) and 6(2) of the Bill.

[5] Clause 6(1) of the Bill uses the word "shall", implying that the Minister must issue a warrant if he has the requisite reasonable grounds for belief.

[6] These grounds for issuing a warrant are set out in clause 6(1) of the Bill.

[7] That is to say, a serious offence as defined in the Serious Offences (Confiscation of Profits) Act [*Chapter 9:17*].

mation-gathering process needed to avert an actual or potential threat to national security or public safety.

Clause 6(3) extends the Minister's powers considerably by allowing him to issue directives to service providers (i.e. operators of postal and telecommunication services) dealing with matters other than the interception or monitoring of communications. What these other matters might be is not stated.[8]

Clause 7 of the Bill imposes some restrictions on the scope of Ministerial warrants. They will be valid for only three months, though they may be renewed for further one-month periods. And they must specify the name, address and other necessary details of the "interception subject" (i.e. the person whose communications are to be intercepted under the warrant). This means that the Minister will not be allowed to issue warrants for the interception of communications generally — for example, a warrant to intercept all communications passing through the system of a particular internet service provider — since at least one of the parties to the communications must be named in the warrant.

Service providers (i.e. operators of postal and telecommunication systems, including internet service providers) will presumably have to comply with Ministerial warrants issued under clause 6 — there is no direct statement in the Bill that they must do so — but whether or not they comply they will not be allowed to tell the interception subject or interception target (the terms are used interchangeably in the Bill to mean the person whose communications are to be intercepted) that a warrant has been issued.[9] In any event they will be obliged to install equipment to allow interception and monitoring to be effected secretly, without the interception subject being aware that it is taking place, and to give Government agents access to communications to and from all interception subjects.[10] For providing this assistance they will be entitled to compensation at a level prescribed by the Minister.[11]

Key-holders, that is to say people who possess the means of deciphering encoded information, will be obliged to decipher the information if required to do so by an authorised person,[12] but they will not, apparently, be obliged to disclose the means (i.e. the key) by which they decipher the information. The obligations of key-holders under the Bill do not seem to be restricted to deciphering information which is the subject of a Ministerial warrant; in other words, a key-holder may be required to decipher any information whatsoever if an authorised person thinks it necessary in the interests of national security or the economic interests of Zimbabwe, or to prevent or

---

[8] Interestingly, there is no express statement that service providers must comply with the Minister's directives, or that they will commit an offence if they fail to do so.

[9] This is the clear implication of clause 9(1)(i) of the Bill.

[10] Clauses 9 and 12 of the Bill.

[11] Clause 13 of the Bill.

[12] See clause 11 of the Bill. An authorised person, as indicated earlier, is defined as meaning the Chief of Defence Intelligence, the Director-General of the C.I.O., the Commissioner of Police or the Commissioner-General of the Zimbabwe Revenue Authority, or a nominee of any of those officers.

detect a serious offence.[13] Key-holders who provide assistance to authorised persons will be entitled to compensation at a prescribed level.[14]

The detention of articles sent by post is dealt with separately, in Part IV of the Bill. Under this Part any postal article will be liable to detention and examination under the authority of a detention order issued by the Minister on the application of an authorised person. The grounds on which the Minister may issue a detention order are stated more widely than those justifying the issue of a warrant under clause 6; a detention order may be issued if there are reasonable grounds to suspect that the postal article concerned contains anything in respect of which an offence[15] is being committed or attempted, or that it contains evidence of the commission of an offence, or that it is being sent to further the commission of an offence, or that it needs to be examined in the interests of defence, public safety or public order.

It is not clear if postal articles will be liable to interception under a Ministerial warrant issued in terms of clause 6 of the Bill as well as being liable to detention and examination under Part IV, or if it is intended that they should be covered exclusively by the provisions of Part IV. Clauses 5 and 6 of the Bill deal with the interception of communications, and the word "communication", though not defined, is clearly intended to cover postal communications[16] — which suggests that postal articles may be intercepted under those clauses. On the other hand, there seems no point in allowing postal articles to be intercepted under a warrant if they can be detained and examined under a detention order issued in terms of Part IV on wider grounds than those justifying the issue of a warrant.

Clause 8 of the Bill states that evidence obtained through illegal interception will not be admissible in criminal proceedings unless the court, having regard to the circumstances and the interests of fairness, allows it to be admitted. This clause is noteworthy in two respects. Firstly, the general rule is that evidence that has been obtained illegally is admissible though the court has a discretion to exclude it on the ground of unfairness or public policy.[17] Clause 8 reverses this rule. Secondly, the clause applies only to criminal proceedings. In civil proceedings, one assumes, the general rule will continue to apply, as codified by section 48 of the Civil Evidence Act [*Chapter 8:01*].[18] It is not clear why the general rule was altered only in regard to illegally-intercepted communications and only in criminal proceedings. If the general rule was thought to be inadequate or wrong, it should have been reversed or abolished in regard to all illegally-obtained evidence and all legal proceedings.

Finally, clause 18 of the Bill gives a right of appeal to persons aggrieved by warrants, directives or orders issued under the Bill. The appeal will lie in the first in

---

[13] See clause 11(1)(b) of the Bill. Note that the grounds on which an authorised person may require information to be deciphered by a key-holder are different from the grounds on which the Minister may issue a warrant under clause 6. There is no reference in clause 11(1) to public safety or a threat to Zimbabwe's international relations.

[14] Under clause 13 of the Bill.

[15] Any offence, it should be noted, not just a serious offence.

[16] See footnote no. 1 above.

[17] See Hoffmann & Zeffertt *The S.A. Law of Evidence* 4th ed pp 278–287, *Kelly v Pickering* 1980 ZLR 44 (A) at 47 C–D, and *Shell (SA) (Edms) Bpk v Voorsitter, Dorperraad van die OVS* 1992 (1) SA 906 (O).

[18] See Hoffmann & Zeffertt *The S.A. Law of Evidence* 4th ed pp 291–2 and *Shell (SA) (Edms) Bpk v Voorsitter, Dorperraad van die OVS* 1992 (1) SA 906 (O).

stance to the Minister and then, if the appellant remains dissatisfied, to the Administrative Court. This clause is rather specious. It will give service providers an avenue by which they may have their grievances settled by a court, but one wonders why they should have to note their appeals to the Minister before approaching the court, particularly in cases where it is the Minister's own decision that is the subject of the appeal. And the clause will give no effective remedy to members of the public whose communications have been intercepted, since they will not be aware of the interception.

CONSTITUTIONALITY OF THE BILL

Is the Bill constitutional?

Section 20(1) of the Constitution guarantees freedom of expression in the following terms:

> "(1) Except with his own consent or by way of parental discipline, no person shall be hindered in the enjoyment of his freedom of expression, that is to say, freedom to hold opinions and to receive and impart ideas and information without interference, and freedom from interference with his correspondence."

Subsection (2) of section 20 allows the right to freedom of expression to be restricted on various grounds, in particular:

> "(a) in the interests of defence, public safety, public order, the economic interests of the State, public morality or public health;
>
> (b) for the purpose of—
>
> …
>
> (v) in the case of correspondence, preventing the unlawful dispatch therewith of other matter;"

but any such restriction will be invalid if it is shown not to be reasonably justifiable in a democratic society.

Freedom of expression has been called "one of the most precious of all the guaranteed freedoms" and one which, together with freedom of assembly, lies at the foundation of a democratic society.[19] As such, it must be given a generous interpretation, and derogations from the right, even those expressed in the Constitution itself, must be strictly construed.[20] This means that the interests of "defence, public safety, public order" and the other interests specified in subsection (2) of section 20 will not be interpreted widely so as to allow great limitations to be placed on the right to freedom of expression. Any law that limits freedom of expression must be sufficiently precise to enable a person to regulate his or her conduct, knowing with reasonable certainty what the law is and what actions are in danger of breaching the law.[21] And limitations on the right will be struck down if they are "over-broad", that is if they cover not only cases that fall within the terms of subsection (2) but also cases outside it.[22] For example, a law that imposes restrictions on freedom of speech that are reasonable in wartime will be over-broad if it extends those restrictions to peacetime. Finally, any re

---

[19] Per Gubbay CJ in *In re Munhumeso & Ors* 1994 (1) ZLR 49 (S) at 56G and 57A.

[20] See *Nkomo & Anor v Attorney-General & Ors* 1993 (2) ZLR 422 (S) at 432D and *Rattigan & Ors v Chief Immigration Officer & Ors* 1994 (2) ZLR 54 (S) at 57G–H.

[21] See *Chavunduka & Anor v Minister of Home Affairs & Anor* 2000 (1) ZLR 552 (S) AT 561B–D.

[22] Or, as expressed in *Chavunduka*'s case at 568A–569D, if there is a lack of proportionality between the potential scope of the limitation and the "evil" against which it is directed.

striction imposed on freedom of expression must be reasonably justifiable in a democratic society. To determine whether it meets that requirement, it has to be tested against the following criteria: [23]

1. whether the legislative objective is sufficiently important to justify limiting a fundamental right;
2. whether the measures designed to meet the legislative objective are rationally connected to it; and
3. whether the means used (to) impair the right or freedom are no more than necessary to accomplish the objective.

An instructive example of how our courts may interpret the Bill is the case of *Law Society of Zimbabwe v Minister of Transport and Communications & Anor* S-59-03, in which the Supreme Court considered the constitutionality of sections of the Postal and Telecommunications Act [*Chapter 12:05*]. The sections concerned were similar to those of the Bill, and empowered the President to direct that communications should be monitored if in his opinion it was necessary to do so in the interests of national security or the maintenance of law and order. He was also empowered, after consultation with the responsible Minister, to give service providers such directions as he considered to be necessary or expedient in the interests of national security or relations with foreign states. The Law Society challenged these provisions on the ground that they afforded no protection to legal practitioner and client privilege. The Supreme Court found them to be unconstitutional, and in its judgment said:[24]

> "The impugned sections 98(2) and 103 of the Act confer on the President unfettered powers to intercept correspondence and communications. The only limitation to the exercise of that power is that the President has to hold the "opinion" that it is necessary in the interests of national security or necessary for the maintenance of law and order. It is not a legal requirement that the holding of the opinion be based on reasonable grounds or good cause. In terms of s 103 of the Act the only restriction on the President before he gives certain directives is that he should consult the Minister, an appointee of the President, who is accountable to him.
>
> Sections 98(2) and 103 of the Act have no built-in mechanism restricting or limiting:-
>
> (a) who the President may authorise to make the interception;
>
> (b) what is to become of the mail or other communication once it has been intercepted;
>
> (c) who has access to the contents in the intercepted communication;
>
> (d) what steps are to be taken to ensure that any lawyer-client privilege is not unduly interfered with.

---

[23] See *Nyambirai v NSSA & Anor* 1995 (2) ZLR 1 (S) at 13B-E. In *Capital Radio (Pvt) Ltd v Broadcasting Authority of Zimbabwe & Ors* S-128-02 at p 46 of the cyclostyled judgment, Chidyausiku CJ added that the presumption of constitutionality had to be borne in mind when determining whether a law was reasonably justifiable in a democratic society, and went on to say that a court has to be satisfied that a statutory provision is arbitrary, oppressive and, consequently, not justifiable in a democratic society before striking it down as unconstitutional. On the other hand, in a later case (*Association of Independent Journalists & Ors v Minister of State for Information & Publicity & Ors* S-136-02 at p 19 of the cyclostyled judgment) the learned Chief Justice applied the three criteria quoted above without adding any riders to them.

[24] At pages 12 and 13 of the cyclostyled judgment.

> The net effect of the failure to provide statutory mechanisms to control or limit the exercise of the power conferred by the Act on the President leads to an unfettered discretion to intercept mail and communication. The impugned sections provide no guidance as to what a citizen should not do to avoid conduct that might lead to the exercise of the powers conferred by the impugned sections. The Act provides no legal recourse or safeguard for the innocent. The Act does not provide any mechanisms for accountability. Similar legislation in other jurisdictions provides or is required to provide, for prior scrutiny, independent supervision of the exercise of such powers and effective remedies for possible abuse of the powers. The Act provides for no such safeguards.
>
> The issue here is not that the powers have been abused or are likely to be abused by the President but rather that there are no mechanisms in the Act to prevent such an abuse. In the absence of such limitations and control mechanisms the powers conferred on the President are too broad and overreaching to be reasonably justified in a democratic society. The impugned sections, as I have already stated, are so vague that the citizen is unable to regulate his conduct in such a way as to avoid the interception of his mail or communication. Thus, in this regard, the impugned sections of the Act are too vague and do not satisfy the constitutional requirement of 'provided by law'."

In the light of these considerations, is the Bill consistent with section 20 of the Constitution?

The first point to note is that although it will permit the interception of communications in the interests of public safety, public or national security and the economic interests of the State, it will go further and allow interception if a serious offence has been or is likely to be committed or if there is a "threat to the national interest involving the State's international relations or obligations". These grounds are not covered by section 20. The term "serious offence" is defined by reference to the Serious Offences (Confiscation of Profits) Act, as noted above, and includes:

- any offence punishable by imprisonment for 12 months or by a more severe punishment;
- an offence where the property involved exceeds $2 million;
- an offence involving narcotics where the property involved is worth $20 000 or more.

So communications will be subject to interception under the Bill for the purpose of detecting or thwarting such crimes as assault, bag-snatching,[25] contempt of court, and possession of a few twists of mbanje or dagga. It should be noted, too, that postal articles will be liable to detention under Part IV of the Bill if they contain evidence of a criminal offence, or if they afford evidence of a criminal offence — any offence, no matter how trivial. Section 20 of the Constitution limits the grounds for interference with freedom of expression to the interests of "public safety, public order, the economic interests of the State, public morality or public health. The term "public safety" means the safety of the community from external and internal dangers, and "public order" is synonymous with public peace, safety and tranquillity.[26] To allow communications to be intercepted or detained for the detection of any offence, or to protect Zimbabwe's international relations, goes far beyond this.

In so far as the grounds for intercepting communications go beyond those set out in section 20 of the Constitution, i.e. in the interests of defence, public safety, public

---

[25] Where the bag contains more than $2 million dollars, which is by no means uncommon in Zimbabwe nowadays

[26] *In re Munhumeso & Ors* 1994 (1) ZLR 49 (S) at 64C–D.

order, the economic interests of the State, public morality or public health, the Bill is over-broad and clearly unconstitutional.

Another ground for impugning the Bill is that it will exert an unduly "chilling effect" on freedom of expression, far beyond what is necessary to protect defence, public safety, public order or the economic interests of the State.[27] Ordinary members of the public will be reluctant to send e-mails, or to send letters through the post, or to make telephone calls, if they believe that their messages are liable to be monitored by government officials. Any e-mail, letter, telephone call or other communication will be liable to interception under the Bill on mere suspicion, even if the suspicion has to be based on reasonable grounds — and in that regard it must be remembered that since the senders and recipients of the communication will be unaware that it is being intercepted, there is no mechanism under the Bill for the reasonableness of the suspicion to be tested. There is no provision, for example, for a warrant to be scrutinised by a judicial officer before it is issued.

Yet another ground on which the Bill is unconstitutional is the one which aroused the concern of the Law Society in the case of *Law Society of Zimbabwe v Minister of Transport and Communications & Anor* cited above: there is no protection for legal practitioner and client privilege. Although the Supreme Court held that the privilege was not specifically protected under the Constitution, but was subsumed under the right to freedom of expression, the learned Chief Justice did observe:

> "I have no doubt that a breach of the lawyer-client privilege almost invariably leads to the violation of one's entitlement to a fair trial guaranteed under s 18 of the Constitution."[28]

And, again as noted above, he listed the fact that there was no mechanism in the impugned legislation to protect lawyer-client privilege as one of the grounds on which the legislation under consideration was unconstitutional.

EFFECT OF THE BILL ON HUMAN RIGHTS GENERALLY

Even if the Bill is found to be constitutional it is likely to have a deleterious effect on human rights. Freedom of expression lies at the foundation of every democratic society and is one of the basic conditions for the progress of democracy. The Bill will inhibit the free exchange of news and opinions, particularly on matters of a political nature. No one will be able to send an e-mail or letter, or make a telephone call, without the fear, however slight, that it will be intercepted by a government agent.

The Government will undoubtedly argue that legislation for the interception of communications is needed to combat international terrorism and crime, and that other democratic countries have enacted legislation for that purpose. The first point may well be true, and the second certainly is, but even if those points are conceded the Bill still gives cause for concern.

As already noted, the grounds on which a warrant may be issued are painted with a very broad brush in clause 6 of the Bill: the fact that a serious offence has or will be committed (without any necessary link between the offence and the communications to be monitored); that it is necessary to gather information concerning a threat to "any compelling national interest"; that there is a threat to the national interest involving

---

[27] Compare *Chavunduka & Anor v Minister of Home Affairs &* Anor 2000 (1) ZLR 552 (S) and *S v Tsvangirai* 2001 (2) ZLR 426 (S).

[28] Pages 7 and 8 of the cyclostyled judgment.

international relations — all these cover an alarmingly wide range of circumstances. Add to this the Minister's power under clause 6(3) to give "any directive" to service providers, the nature and scope of such directives being unstated, and the State's control of communications becomes enormous. Does the immediate threat of international terrorism or crime to Zimbabwe justify such extensive limitations on freedom of expression? In the absence of any convincing and publicly-stated justification for the Bill, there remains a suspicion that the Government wants the Bill in order to monitor and forestall the legitimate political activities of its opponents.

Other countries have legislation that allows communications to be monitored, certainly, but their legislation is more limited than the Bill. The British Regulation of Investigatory Powers Act 2000, for example, allows a Secretary of State to issue warrants for the interception of communications, but his actions are subject to monitoring and review by an independent official, the Interception of Communications Commissioner. And while the government of the United States can require telecommunications service providers to maintain equipment that permits the interception of communications under the Communications Assistance for Law Enforcement Act of 1994, it is subject to monitoring by the courts and Congress. There are no such safeguards in the Zimbabwean Bill.

The point should also be made that when a democratic government which generally respects the rights of its citizens introduces legislation that permits invasions of privacy, there is generally less cause for concern than when similar legislation is introduced by a despotic government which has a record of violating the rights of everyone, citizens and non-citizens alike.

B.D. Crozier.

28 July, 2006