Interception of Communications Bill: An analysis of the situation in other jurisdictions

By Wilbert P. Mandinde

The government of Zimbabwe on 26 May 2006 gazetted the Interception of Communications Bill (hereinafter, the Bill).

In coming up with a Bill of this nature, Zimbabwe has not necessarily scored a first as other countries both in Africa and in other continents have such legislations in place. However, most of these countries regulate the interception of communications through constitutional provisions protecting the privacy of communications, and requisite laws and regulations to implement the constitutional requirements. Australia, New Zealand, Canada and Hong Kong have adopted a privacy protection regime that involves the use of Privacy Impact Assessments. It is worthy noting that save for South Africa, African initiatives relating to privacy have been limited. Privacy regimes are under-developed in Africa resulting in communal considerations over-riding individual privacy in the absence of protective legislation.

The preamble of the Bill states that the bill aims to regulate the authorised monitoring and interception of communications. It further aims to provide for the interception of postal articles and communication. It will further prohibit the provision of telecommunication services that do not have the capacity to be monitored. The South African Interception and Monitoring Act (hereinafter the SA Act) also has similar provisions. The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 published in the Government Gazette on 22 January 2003 compels service providers to retain personal data that they have collected from customers indefinitely, and make it available to law enforcement agencies when requested to do so.

HUMAN RIGHTS AND ELECTRONIC SURVEILLANCE

It is recognised worldwide that wiretapping and electronic surveillance is a highly intrusive form of investigation that should only be used in limited and very exceptional circumstances. Nearly all major international agreements on human rights protect the rights of individuals from unwarranted intrusive surveillance.

Article 12 of the 1948 Universal Declaration of Human Rights states:

> *No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks on his integrity or reputation. Everyone has the right to the protection of the law against such interferences or attacks.*

This provision is entrenched under Article 17 of the International Covenant on Civil and Political Rights, which went into force in 1966. The United Nations Commissioner on Human Rights in 1988 made it clear that this broadly covers all forms of communications.

> *Compliance with Article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.*

A number of the regional human rights treaties also legally enforce these rights.

The African [Banjul] Charter on Human and Peoples' Rights was adopted on 27 June 1981. Zimbabwe is a party to this Charter, which unfortunately omits the right to privacy for individuals, leading scholars to conclude that Africans do not value individual privacy.[1]

However Article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms states:

> *Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society 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, of morals, or for the protection of the rights and freedoms of others.*

The European Court on Human Rights has heard numerous cases on the right of the privacy of communications. It has ruled that countries must adopt laws regulating electronic surveillance by both governments and private parties and set out guidelines on the protections that countries must follow.

Article 11 of the American Convention on Human Rights sets out the right to privacy in terms similar to the Universal Declaration. In 1965, the Organisation of American States proclaimed the American Declaration of the Rights and Duties of Man, which called for the protection of numerous human rights, including privacy. The Inter-American Court of Human Rights has begun to address privacy issues in its cases.

The right of privacy of communications is also equally recognised at the national level worldwide. Nearly every country in the world recognises privacy as a fundamental constitutional human right either explicitly or implicitly.

SCOPE OF THE WARRANT FOR INTERCEPTION OF COMMUNICATION

Section 7 of the Bill deals with the scope of the warrant for communications interception. In terms of that section, a warrant should set out the premises in relation to which the

[1] See Lee. A. Bygrave; 'Privacy Protection in a Global Context-A Comparative Overview', Scandinavian Studies in Law, 2004, Vol. 47, p 319-348.

interception shall take place and all the necessary details relating to the interception target.

The surveillance laws of most democracies either specifically define which crimes electronic surveillance may be used to investigate (See e.g. US law at 18 U.S.C. § 2516) or limit it to crimes that impose a certain level of penalty. The Netherlands requires crimes that impose imprisonment of at least 4 years. In Australia, the minimum is seven years. In national security cases, it usually must be proven that the target is acting on behalf of a foreign government or organisation (See U.S. Foreign Intelligence Surveillance Act 50 U.S.C. §§ 1801-11) or an organisation that poses a serious threat to the government of the country.

This ensures that legitimate and normal activities in a democracy such as journalism, civic protests, trade unionism and political opposition, are not subjected to unwarranted surveillance because the individuals involved have different interests and goals than of those in power. It also ensures that relatively minor crimes, especially those that would not generally involve telecommunications for facilitation, are not used as pretexts to conduct intrusive surveillance for political or other reasons.

STANDARDS FOR SURVEILLANCE ORDERS

In terms of Section 5(2) of the draft Bill, an application for lawful interception shall be made to the Minister. The persons who are authorised to make applications for interception of communication are:

- The Chief of the Defence Intelligence
- The Director-General of the President’s department of national security
- The Commissioner of Police
- The Commissioner-General of the Zimbabwe Revenue Authority.

For the Minister to consider the application, it shall contain the following information prescribed in Section 5(3):

(a) name of person whose communication is required to be intercepted.

(b) name of postal service or telecommunications provider to whom the direction must be addressed.

(c) full particulars of all facts and circumstances alleged by the applicant.

(d) indicate whether other investigative procedures have been applied and have failed to produce the required evidence or must indicate the reason why other investigative procedures reasonably appear to be unlikely to succeed if applied or are likely to be dangerous to apply in order to obtain the required evidence.

In South Africa, an application is made to a judge who is required to only be "satisfied" that, "there are reasonable grounds to believe" before authorising surveillance. This is

done to establish an adequate threshold to prevent its use in questionable or marginal cases.

Most other democratic countries' laws require a higher standard. In English-language countries, "probable cause" or a similar level of finding is generally required.

In the UK, authority to intercept communications can only be given by the Secretary of State personally. Where the warrant is the result of a request for assistance made under an international mutual assistance agreement and where the subject or premises to which the interception relates appear to be outside the United Kingdom, a senior official may give authority. Such authority can only be given to those persons specified in Section 6(2) of the Regulation of Investigatory Powers Act 2000. They are:

- the Director-General of the Security Service;
- the Chief of the Secret Intelligence Service;
- the Director of the Government Communications Head Quarters;
- the Director-General of the National Criminal Intelligence Service;
- the Commissioner of Police of the Metropolis;
- the Chief Constable of the Royal Ulster Constabulary (now the Police Service of Northern Ireland);
- the chief constable of any police force maintained under or by virtue of section 1 of the Police (Scotland) Act 1967;
- the Commissioners of Customs and Excise;
- the Chief of Defence Intelligence; and

a person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the United Kingdom.

Further, authority can only be given where the Secretary of State is satisfied that the interception is necessary:

- (a) in the interests of national security;
- (b) for the purpose of preventing or detecting serious crime;
- (c) for the purpose of safeguarding the economic well being of the United Kingdom;
- (d) in circumstances where he would issue a warrant under (b) above, to give effect to an international mutual legal assistance agreement.

In the United States, it is necessary to state that one of the crimes that electronic surveillance is authorised for is being committed; the identity of the location and persons

being targeted; certification that normal investigative procedures have been tried and failed, or are likely to fail or are too dangerous; and a promise to minimise the interception of conversations to only those relevant to the investigation. Other countries including Canada and New Zealand have similar procedural requirements.

In Uganda, law enforcement agents usually require information as part of surveillance which is largely due to suspicions or investigations relating to offences such as threatening violence, robbery and terrorism in which telecommunication devices are used as well as the theft of telecommunications handsets. The court orders are requested for by the Criminal Investigations Department and other agencies such as the Inspectorate of Governance in whom investigative the law vests powers.

Wire-tapping and electronic surveillance are invasions into communication privacy and these are usually occasioned by private-investigative firms, telecommunications operators, service providers who have the capacity to look at what they transmit and public-law enforcement agencies such as the police particularly the Criminal Investigations Department and the Inspectorate of Government. The Judiciary has participated in this process by issuing court orders, which authorise telecommunication companies to release traffic data. Such orders are based on provisions made in the law. In Uganda the rules or principles of privacy and guidelines concerning interception on the basis of law enforcement or intelligence gathering have not been developed which may culminate in abuse.

Unlike other countries, Uganda lacks wiretap law with express provisions on how the surveillance is to be conducted.

Consumer protection agencies have not come up to address privacy concerns, as they tend to focus on quality and standard of goods.

ESTABLISHMENT OF AN INDEPENDENT COMMISSION

Under Section 4 the Bill establishes a Monitoring of Interception of Communications Centre. Section 4(3) establishes that the centre shall be manned, controlled and operated by designated technical experts from the MICC. Technical and other staff within the service providers and the monitoring centres have access to highly sensitive information and are vulnerable to approaches by criminals and others determined to know whether their communications are being monitored and/or demanding access to the content of monitored communications. Staff who have access to intercept-related information should undergo a vetting procedure.

Initial indications are that state security agents will man the Centre. However, it is important to note that such a sensitive issue has to be handled by an independent commission.

An independent commission should be established to oversee all monitoring and interception activities. Independent commissions have been established in many nations that have implemented surveillance laws, such as Australia, New Zealand and Britain.

The commissions ensure that only the communications of the suspect are intercepted and sent through to the monitoring centres, and that communications of a suspected party are methodically intercepted and time-stamped to ensure evidential integrity. The commission undertakes a full and public reporting process; the report can be presented in such a way as to not compromise the information.

The need for such a commission is especially critical in a developing country context where people have concerns about trusting those in power. It will also curb the potential for abuse within the communication monitoring centres, and ensure that accidental interceptions of unwarranted communications are reported and minimised.

COSTS

The Bill requires that industry providers bear the costs of upgrading and maintaining their networks to make them capable of interception. The SA Act also makes any communication service that cannot be monitored by the authorities illegal, and gives the Minister of Communications broad powers to specify technical and security requirements, facilities and devices as well as the type of communication-related information to be stored.

This will result in increased surveillance, a stifling of innovation, reduction of the availability of services, and higher costs on consumers. Industry commentators in many countries around the world have consistently asked for the inclusion of a reimbursement requirement, and the private sector has supported such requests.

Requiring that law enforcement agencies pay for their surveillance capabilities provides an important level of accountability through the budget process. The lack of reimbursement significantly lowers the barriers to law enforcement surveillance by removing budgetary limits that would require that new surveillance capabilities be cost effective before they are implemented. Without it, it has been the experience in many countries that law enforcement places unreasonable demands on providers for expansive surveillance capabilities without justifying their demands.

Service providers in acquiring the necessary equipment for interception, providing technical maintenance thereof, can incur significant costs in meeting the running operating costs. This has been a contentious issue in other countries that have dealt with the same issues that have not been easily resolved.

An alternative approach would entail making the service provider responsible for the monitoring of information on its communication networks to cover the costs. Some argue that this brings exorbitant and unfair expenses on the Internet and telecommunications industries particularly at a time when the international economy is experiencing a downturn in these sectors.

The Netherlands serves as an illustrative example. The Netherlands Telecommunications Act places the responsibility for the cost of acquiring and maintaining interception technologies on the service providers. In February 2001, up to a third of Dutch Internet Service Providers (ISPs) were facing bankruptcy due to the high costs of mandatory Internet traffic interception and due to the technical difficulties and the high costs

involved, ISPs were unable to make their systems interceptable by the deadline date of 15 April 2001

Others argue that the current software utilised by many of the larger service providers already has the routing capabilities required for interception. Smaller service providers would incur costs, but there are appropriate solutions to help them defray the expense. For example, British legislation holds that the Government will cover "reasonable costs" incurred by the smaller ISPs in ensuring that their services conform to the legislation.

There is concern that the Bill will place onerous demands on smaller ISPs and that the growth of the industry will be affected at a time when access to communication services needs to be actively expanded. The demise of smaller service providers can have a detrimental effect on the overall economy and the integration of ICTs into society, especially within a developing country context. The imposition of these requirements will be difficult and very expensive. Most equipment does not come with the capability for surveillance, so no off-the-shelf solution is available.

While it is argued that a market for technologies with embedded surveillance capabilities may emerge and reduce the costs, there are three intertwined problems inherent in this argument. First, particularly within ISPs, each network is very different and introducing these technologies may harm the effectiveness and efficiency of the networks. Second, these technologies are being developed within strict standards regimes. Meanwhile the Internet Engineering Taskforce (IETF), a relatively open body, has refused to develop such technologies.

And third, such a market has failed to emerge, perhaps because of the technical burdens and substantial public opposition in many countries to facilitate increased electronic surveillance.

Countries that have attempted to impose wholesale the law enforcement costs on the industry have seen delays and loss of new companies and jobs. In the Netherlands, the Telecommunications Act imposes a similar burden on providers as envisaged under the Zimbabwean Bill.

The costs for creating this capability are not compensated by the government.

The government did not assess the probable costs and it was particularly difficult for ISPs to comply, as there is little experience in creating such capabilities in networks. The Industry Organisation of Internet Service Providers in the Netherlands **(NLIP)** has estimated that the costs will be several million Euros, and there are strong concerns as to how this will affect small local and regional ISPs. NLIP expects an increase in the price of Internet access in the Netherlands as a result and a mass closing of small ISPs. After much lobbying, the deadline for lawful interception implementation was delayed for ISPs and it is expected that the majority of the ISPs will not meet the extended deadline.

In Australia, carriers are also obliged to develop and implement at their own expense an interception capability. The costs and burden upon the operators have proven more

difficult and expensive than anticipated. As a result, the carriers were given both a waiver from the requirement for several years and, it is understood, a subsidy towards the cost.

There is also the issue of the unquantifiable opportunity cost. While technological researchers and network experts expend time and resources on interception capability, they are losing time that could be spent researching network efficiency and operations. As a result, the costs incurred by the interception capability work are enormous. A study conducted by Privacy International and the London School of Economics on the economic impact of the UK's wiretap bill concluded that opportunity costs were a major part of the economic costs of the legislation.

LACK OF PUBLIC ACCOUNTABILITY

Another important oversight measure missing in the Bill is a provision requiring the production of annual public reports on the use of electronic surveillance by government departments. This is a common feature of wiretap laws in English-speaking countries and many others in Europe and should be included in the draft law.

Countries that issue annual reports on the use of surveillance include the U.S., U.K., Sweden, Canada, Australia, New Zealand and France. These reports typically provide summary details of the electronic surveillance conducted, the types of crimes authorised for, their duration and other relevant information. In the US, the Administrative Office of the U.S. Courts produces the report and submits it to Congress. In Australia and Canada, an annual report to the Attorney General must be tabled in Parliament. In the UK the Interception of Communications Commissioner publishes the report.

These countries recognise that openness and transparency are essential to limit abuses. They are widely used in many countries by the Parliaments for oversight and also by journalists, NGOs and others to examine activities related to law enforcement.

A number of countries including the United Kingdom and France also have special commissions that review wiretap usage to check against possible abuses. These bodies have expertise that most judges who authorise such surveillance do not have. They also have the ability to conduct follow -up investigations once a case is complete. In other countries, the Privacy Commission or Data Protection Commission also has some ability to conduct investigations on possible oversights of electronic surveillance.

In addition, there are no provisions in the Bill to inform individuals who have had their communications intercepted or their transactional information collected once the investigation has been completed. Nor is there any timetable set for expunging information once it is no longer necessary. This is an important feature found in many laws around the world that provides another level of oversight, especially in those cases where innocent parties' communications are intercepted.

EVIDENTIAL INTEGRITY OF INTERCEPTED INFORMATION

Section 8 of the Bill deals with the inadmissibility of unlawfully intercepted information.

The Bill, however, does not state the processes required to ensure evidential integrity of intercepted information. This should be clearly stated. The entire content of the intercepted message has to be made available to the defence if an intercepted communication is to be used as evidence in a court of law.

It is recommended that the systems and procedures that will be in place to ensure the integrity of the information and prevent evidential tampering be clarified.

RECOMMENDATIONS

The Zimbabwean government, borrowing from other jurisdictions worldwide, should develop a policy to:

(i) ensure that privacy protection is a core consideration in all activities;

(ii) ensure that accountability for privacy issues is clearly incorporated into the duties of all institutions, jurisdictions and sub-sectors;

(iii) provide decision-makers with the information necessary to make fully-informed policy decisions based on an understanding of the privacy implications and risks and the options available for avoiding and/or mitigating those risks;

(iv) promote an awareness of sound privacy practices and also regulate surveillance as other countries such as Australia have done. Law enforcement agencies and other entities require law to guide the conduct of investigations. In Australia, the *Telecommunications Act 1997* includes provisions dealing with the privacy of personal information held by carriers, carriage service providers and others, provisions that embrace the development of voluntary industry codes and standards relating to privacy.

Policies on privacy should among others address:

(v) obligations and other related duties; rights; sanctions and compliance measures;
(vi) enforcement, monitoring and implementation mechanisms;
(vii) institutional framework and collaborative arrangements required implementing the policy.

Departments and agencies must ensure and document that privacy principles, legislation and policies are adhered to and that privacy impacts and risks associated with programme and service delivery activities have been resolved or mitigated.

Disclosures of information should be monitored so as to reveal what information was disclosed, the source of the request, justification and the time.

Law enforcement officers need laws and guidelines to keep them in line with the requirements of privacy laws so as to prevent abuse when conducting investigations. An example could be the UK Regulation of Investigatory Powers Act 2000 discussed above.

There is need for telecommunications companies to develop privacy policies, to raise awareness for customers through consumer organisations and to establish and boost the activities of complaints desks in telecommunications companies with better capacity to address growing needs.

There is need for more education and awareness of privacy vis-à-vis cultural considerations and perceptions of what amounts to privacy.

Capacity building remains crucial especially where it concerns legal issues pertaining to ICTs including privacy concerns. This process involves the development of curriculum at universities and other tertiary institutions and specialised institutions such as the Judiciary, Parliament, human rights bodies, criminal investigation arms and state security agencies. This will cater for the expected demand for human resources and also meet the human resource capacity standards required at all levels.

The constitutionality of privacy-invasive laws has to be determined at all times before policies are passed and reduced to draft laws and passed in Parliament.

Parliament should make a special requirement for the proposed Zimbabwe Human Rights Commission to make a report on the state of privacy in Zimbabwe to be able to develop benchmarks on the basis of which regulators can operate.

CONCLUSION

Overall, the Bill is flawed, as it does not contain basic safeguards against the invasion and unwarranted intrusion into privacy as found in other countries. The Bill represents a step backwards and is inconsistent with international standards on human rights and other legal requirements. On the basis of international experiences, the lack of these essential safeguards to protect the right to privacy will inevitably lead to abuses.

The lack of legal protections in this Bill will invite abuse and have a severe impact on human rights and privacy.

It is recommended that the Bill in question should be subjected to rigorous scrutiny before it is even tabled before Parliament as it has immeasurable inadequacies compared to laws in other jurisdictions which respect the right to privacy.