1 September 2006

Committee Clerk
Parliamentary Portfolio Committee on Transport and Communications
Parliament of Zimbabwe
Harare

Dear Sir/Madam

ZISPA Submission on Interception of Communications Bill 2006

Further to the public hearing on the above Bill on Wednesday 30 August, ZISPA would like to formally present our views on the Bill to your Committee. We appreciate the opportunity given to express our views on this Bill, which raises many issues of concern to the Internet community in Zimbabwe. We therefore hope that these will be taken into account in considering this Bill.

In addition to the points raised in the attached submission, there are two further issues which we would like to deal with. The first is related to the statement made at the hearing by the Director-General of POTRAZ, Dr Chidoori. He indicated that it was not intended to apply the provisions of the Bill to Internet Service Providers, but only to licensed service providers, ie Internet Access Providers. This is a very important issue, as it is certainly not clear from the wording of the Bill that this is the case. We would therefore like to request that the definition of the term "telecommunications service provider" be explicitly clarified in the definitions in Section 2 of the Bill. It should be noted that the Telecommunications Act [Chapter 12:05] is itself unclear in this regard, and it is only the related regulations that define categories of service providers.

Secondly, we would like to point out that a major part of the operation of an Internet e-mail service consists of blocking mail from spammers, hackers, phishing attackers or infected computers sending out worms, viruses and other malware. Between 80 to 90% of all e-mail now consists of undesirable material of this kind, and it is the duty of any responsible ISP to block such traffic. Sometimes we block connections from external servers completely, and at other times we accept the connections but quarantine the content when it is identified as containing malware. Suspect traffic may have potentially dangerous attachments or scripts removed while the message itself is still delivered. We would like reassurance that such activities, which are a bona fide part of the operation of any ISP, are accepted as legitimate forms of interception of communications, as they are carried out for the benefit of our clients, and with their full knowledge.

Yours faithfully

Jim Holland
for ZISPA

Interception of Communications Bill 2006

Comments by ZISPA

Introduction

This document represents the views of ZISPA, the Zimbabwe Internet Service Providers Association, on the Interception of Communications Bill 2006, which is currently before Parliament.

ZISPA understands that in many democratic countries there is legislation that provides a legal basis for the interception of selected communications, in order to protect national security and to investigate criminal activities. Such legislation is frequently controversial, as it has to strike a balance between unfettered monitoring and allowing criminals to roam free, between what is reasonable in a democratic society and what is not.

Background

The proposed Bill follows two previous attempts to legitimise the interception of communications by the government:

- Sections 98 and 103 of the Posts and Telecommunications Act (No 4/2000), which provided for the interception of communications if the President considered it necessary "in the interests of national security or the maintenance of law and order", and for him to give service providers "directions of a general character as appear to the President to be requisite or expedient in the interests of national security or relations with the government of a country or territory outside Zimbabwe."

- A draft amendment to the standard franchise agreement between ISPs and TelOne which included provisions that required service providers to block "objectionable, obscene, unauthorised or any other content, messages or communications infringing copyright, intellectual property right and international and domestic cyber laws, in any form or inconsistent with the laws of Zimbabwe". Service providers were required to "provide, without delay, all the tracing facilities of the nuisance or malicious messages or communications . . . to authorised officers of TelOne and Government of Zimbabwe/State Government, when such information is required for investigations of crimes or in the interest of national security. Cyber Laws as and when framed shall be applicable." It also stated: "The use of

> the network for anti-national activities would be construed as an offence punishable under the Zimbabwe Law or other applicable law."

The Law Society challenged the constitutionality of Sections 98 and 103 of the Posts and Telecommunications Act in the Supreme Court, especially in so far as they potentially violated the right to lawyer/client privilege and the right to freedom of expression. They won the case when the Court ruled in March 2004 that these Sections violated Sections 18 (the right of an accused person to a fair trial) and 20 (the right to freedom of expression) of the Constitution.

With regards to the proposed amendment to the Internet Service Franchise Agreement, the ISPs attempted to seek clarification from TelOne over the wording of the amendment as it seemed extremely broad and undefined in its scope, and referred to "Cyber Laws" that did not exist. As no response was received from TelOne, ZISPA members did not sign the amendment.

Provisions of the Bill

The Interception of Communications Bill states that its purpose is:

> To establish an interception of communication monitoring centre and for the appointment of persons to that centre whose function shall be to monitor and intercept certain communications in the course of their transmission through a telecommunication, postal or any other related service system

The Bill says nothing about the purpose for which the communications shall be intercepted, although it is implicit that the data may be used as evidence in criminal proceedings.

Key provisions of the Bill of interest to telecommunications service providers are:

- The Minister of Transport and Communications may issue warrants for the interception of communications on application by the Chief of Defence Intelligence, the Director-General of the President's Department of National Security (the CIO), the Commissioner of the Zimbabwe Republic Police and the Commissioner-General of the Zimbabwe Revenue Authority or by any nominee of any of the above. The applications should normally be in writing, but in urgent or exceptional circumstances oral applications can be made.

- Warrants may be issued where the Minister has reasonable grounds to believe that "a serious offence has been or is being or will probably be committed or that there is threat to safety or national security of the country" or that "the interests of the country's international relations or obligation(s) are threatened".

- Warrants are valid for a period of up to 3 months but may be extended by further periods of up to a month at a time, indefinitely.

- Service providers are required to install at their own cost "hardware and software facilities and devices to enable interception of communications"; to store communication-related information; to establish connections to the monitoring centre to route the intercepted communications to the centre; and also to store detailed identity information on all their customers.

- Service providers are prohibited from disclosing any information about warrants they receive and communications intercepted except to authorised persons.

- Authorised persons are entitled to order the disclosure of security keys used to protect information where considered necessary on grounds of national security, preventing and detecting crime, and in the interests of the economic well-being of Zimbabwe.

- Penalties for failure to comply with provisions of the Bill range from a fine to from three years to five years maximum imprisonment.

- Aggrieved parties may appeal first to the Minister, and then to the Administrative Court.

Concerns of Service Providers

The Bill raises many issues of concern to Internet service providers, given that it would require them to be involved in the monitoring of e-mail and Web downloads by targeted individuals or organisations. It would also allow any other form of Internet service to be intercepted as well, including instant messaging, VOIP calls (once these are authorised by POTRAZ), and financial transactions in particular.

Specific concerns are:

- **Lack of Judicial Involvement and Oversight**

    - Normal international practice for legislation of this kind is for warrants to be issued as the result of some judicial process, and for provision to be made for an annual review of the implementation of the Act to ensure that its measures are not being abused. Chinese Government legislation recently passed after much criticism in Hong Kong, for example, requires that judges must first approve all surveillance operations.

- There is no provision in the Zimbabwean Bill for any judicial involvement or parliamentary oversight of the implementation of the Act to ensure that it is implemented fairly by the Minister and his officials. Given the Minister's extremely wide discretionary powers to determine whether a warrant may be issued or not, there is the possibility of the current Bill being used to give carte blanche to interceptions. This makes it likely that if this Bill is passed in its current form it could be successfully challenged on constitutional grounds in similar fashion to the provisions of the Posts and Telecommunications Act.

- **Loss of privacy for Internet users**

  - Because of the lack of provisions for judicial involvement or any review mechanism, it appears that private and confidential personal information could be intercepted and misused by officials who obtain access to it. This could include communications between lawyers and clients, doctors and patients, priests and their flock, journalists and their sources, for example. These could all involve completely legal activities but disclosure of information in such communications could cause serious harm to the individuals concerned. While the Bill itself makes such misuse an offence, there is concern that the lack of oversight would make this unlikely to be discovered.

  - Confidential commercial or financial information could be intercepted and abused. This could include tender documents, business plans, personnel data, details of bank transactions etc. In the worst-case scenario, passwords could be intercepted and used for fraudulent purposes.

  - There is a danger of abuse of the provisions of the Bill to target political opponents of the government, or indeed of members of rival factions of the ruling party. NGOs involved in legal lobbying and campaigning also would seem to be at particular risk.

  - There is no guarantee that communications of the targeted subject that are not related to the matters raised in the application for the warrant will not be intercepted, or that communications of totally innocent third parties will not be intercepted at the same time.

- **Lack of Clarity of Bill**

  - The Bill is very vague in its provisions, and extremely broad in scope, without precise definitions of terms such as "national security", "national economic interests", "interests of the country's international relations or obligations" or "economic well being of Zimbabwe".

- Warrants can be issued to intercept communications even when no criminal activity is suspected, but simply on political grounds such as when "the interests of the country's international relations or obligations are threatened". This means that any organisation involved in legal international lobbying that the government does not approve of could be targeted.

- The Bill will stifle the use of the Internet in Zimbabwe because of its vagueness and broad scope. It will frighten people from undertaking perfectly legal communications that they fear could be intercepted and used against them. In the past this fear has resulted in chain letters asking people not to forward any e-mails with political comment or political jokes. Would such communications on topics that are freely published in newspapers be regarded as legitimate targets of interception under this Bill?

- Service providers are not going to be able to assure their clients that normal personal and business communications will be free from interception and possible abuse, to the detriment of secure financial transactions in particular, and indeed are not even going to be able to advise their clients on what they should not be doing to avoid becoming subject to the provisions of the Bill.

- **Technical and Financial Difficulties in Implementation**

  - Service providers are going to have to bear the potentially extremely high capital and forex costs of the necessary hardware and software. By contrast, under South African legislation, there is provision for the state to bear the cost of purchase of equipment that is placed in a pool from which it is then issued to specific providers when a warrant is issued. Estimated costs for such equipment are of the order of 1 million USD upwards, depending on the size of the ISP. Costs of this order would put all local ISPs out of business, even if the foreign currency necessary were available for purchase.

  - In addition to the costs of procurement of necessary hardware and software, service providers would also have to train technical staff in its operation and allocate them to these extra duties, to the detriment of their normal operations.

  - Depending on the type and configuration of the equipment installed, it could be possible for it to be fully managed from the proposed communication monitoring centre, thereby leading to even more possibilities for abuse as there would then be no technical reason for warrants to be issued on service providers once such equipment was in place - all communications could be monitored regardless. A basic safeguard would be for the monitoring equipment to be set up at a particular ISP only when a warrant has been issued, and for the equipment to be configured specifically to monitor only the communications of the target of that warrant. Once the period of the warrant has expired then the equipment should be removed.

- Service providers are going to have to undertake the massive and expensive task of obtaining and maintaining detailed identification details for all their current and future clients. The value of such information is also questionable, given that an account issued in one person's name can be used legitimately by anyone else that that person chooses to allow to access it. What about a single corporate account that could be used by hundreds of staff members? Or an Internet Café that is used by hundreds of different people every day?

- There are no details provided as to what communications data will have to be stored by service providers, and for how long. Depending on the volume and timescale, such data storage could impose considerable cost burdens.

Conclusions

ZISPA's key objective is to see the growth and development of the Internet in Zimbabwe. We face many difficulties due to inherent problems such as the lack of foreign currency, skills shortages, poor reliability of the phone system, electrical power outages etc. We are concerned that this Bill will further constrain the development of this important sector that is so vital for the growth of this country. The Bill will increase the technical and financial burdens on the sector, adding to general demoralisation, and deterring investment, especially in the area of e-commerce. As a result, the country will continue to lag even further behind its competitors in many areas, not just this specific sector. Economic growth is dependent on a viable and competitive telecommunications sector.

The effectiveness of the Bill in combating serious crime is also questioned, given that those involved in such activities are likely to use encrypted communications that are simple to set up but extremely difficult to crack without having access to days of processing time on supercomputers not available in this country.

ZISPA would like to work with Government to ensure that appropriate legislation is developed that does meet the needs for national security and crime prevention while also ensuring that it enhances the needs of the sector (especially in areas such as ensuring the security of communications, including e-commerce specifically, and the protection of computer networks).

Zimbabwe has the opportunity to create legislation that takes into account the experiences of other countries while at the same time ensuring that it meets the requirements and conditions of the situation on the ground.

Recommendations

ZISPA recommends that the Interception of Communications Bill 2006 be withdrawn in its present form and that a new Bill be drafted following:

- Well-publicised public meetings to obtain feedback from affected parties
- Detailed discussions with key stakeholders in the sector
- A study of similar legislation and its implementation in other countries

Nikki Lear
Acting Chairperson
ZISPA
Harare
August 2006