



PRIVACY INTERNATIONAL

August 13, 2001

Committee on Justice & Constitutional Development
c/o The Secretary to Parliament
PO Box 15
Cape Town 8000
South Africa

Attn: Ms Collette Herzenberg or Ms. Zodwa Zenzile

RE: Comments on Interception and Monitoring Bill

We are writing in response to your solicitation for comments on the Interception and Monitoring Bill currently being reviewed by the Committee. These comments are submitted on behalf of Privacy International, a human rights group dedicated to the protection and promotion of individuals' privacy interests worldwide.

PI represents member organizations and individuals from a wide variety of backgrounds specializing in privacy, surveillance, data protection and freedom of information in over 40 countries and has offices in London and Washington, D.C. PI engages in a wide variety of educational and other activities each year including testifying before many national and international bodies, organizing campaigns, issuing reports, holding conferences, and co-producing the annual international survey on Privacy and Human Rights (available at <http://www.privacyinternational.org/survey>). The organization and its members have been actively involved in deliberations and campaigns on electronic surveillance in many jurisdictions worldwide for over 10 years.

Overall, we find the bill lacking many basic safeguards found in other countries' laws. We believe that the bill represents a step backwards from the Interception and Monitoring Prohibition Act 1992 and is inconsistent with international standards on human rights and the legal requirements of the South African Constitution. On the basis of international experiences, we believe that The lack of safeguards will inevitably lead to abuses.

We recognize South Africa concerns over the issue of crime but the bill threatens to undermine democratic principles enshrined in the South African Constitution and is

WASHINGTON OFFICE
1718 CONNECTICUT AVE, NW, SUITE 200 • WASHINGTON, D.C. • 20009
PHONE: (202) 483-1217 • FAX: (202) 483-1248 • pi@privacy.org
<http://www.privacyinternational.org>

likely to reduce South African citizens' confidence in their government because of its broad powers and lack of protections.

We recommend that the Committee refrain from approving this bill until these issues are addressed. Our specific comments are outlined below.

HUMAN RIGHTS AND ELECTRONIC SURVEILLANCE

It is recognized worldwide that wiretapping and electronic surveillance is a highly intrusive form of investigation that should only be used in limited and unusual circumstances. Nearly all major international agreements on human rights protect the right of individuals from unwarranted invasive 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 honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.

This language was adopted into Article 17 of the International Covenant on Civil and Political Rights, which went into force in 1966. The U.N. Commissioner on Human Rights in 1988 made 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.¹

A number of the regional human rights treaties make these rights legally enforceable. 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. (2) 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.

¹ United Nations Human Rights Commissioner, The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17). 08/04/88. CCPR General comment 16.

The European Court of 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 Organization 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 recognized on the national level worldwide. Nearly every country in the world recognizes privacy as a fundamental human right in its constitution, either explicitly or implicitly.² Most include secrecy of communications.

LACK OF DEFINITION FOR SURVEILLANCE CONDUCTED FOR REASONS OF “COMPELLING NATIONAL INTEREST”

One of the most troublesome aspects of the bill is the broad allowance for surveillance allowed under Article 4. The scope for authorizing surveillance under this section does not include meaningful limitations to prevent abuses.

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 organization (See U.S. Foreign Intelligence Surveillance Act 50 U.S.C. §§ 1801-11) or an organization that poses a serious threat to the system of government of the country.

This ensures that legitimate and normal activities in a democracy such as journalism, civic protest, trade union organizing and political opposition are not subjected to unwarranted surveillance because the individuals involved have different interests and goals than 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.

In contrast, Article 4(2)(b) authorizes surveillance to protect the “security or other compelling national interest” without defining it or placing any limitations on that broad discretion. Article 1(g)’s definition for surveillance of “serious crime” for 4(2)(a) repeats

² See US Department of State, Country Reports on Human Rights for 1996, 1997 (Privacy Excerpts) <http://www.privacy.org/pi/reports/hr96_privacy_report.html>.

that authorization as an additional justification for surveillance under that section without further defining its scope.

LOW STANDARD FOR SURVEILLANCE ORDERS

The standard set out in Article 4(2) that a judge is required to be only be “satisfied” that, “there are reasonable grounds to believe” before authorizing surveillance establishes an inadequate 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. The standard proposed would appear to be below what is required under Section 36 of the South African Constitution.

In addition, the procedures set out under 4.2(a) that a judge only is required to determine that the offense “cannot be investigated in appropriate manner” provide little protection. Under 4(2)(b), even that minor finding is not required. This is a considerably lower level of protection than found in many other democratic countries that generally require detailed findings before an authorization can be issued. For instance, in the United States, 18 U.S.C. § 2518 requires: a statement that one of the crimes that electronic surveillance is authorized 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 minimize the interception of conversations to only those relevant to the investigation. Other countries including Canada and New Zealand have similar procedural requirements.

TECHNICAL STANDARDS AND REQUIREMENTS

This bill imposes significant burdens on an extremely wide range of private persons, organizations and companies. There are few, if any, computer or communications systems that would not fall under this definition. Every new communications tool and system would be required to implement surveillance capabilities.

We are very concerned about the impact of Article 7(1) which prohibits all telecommunications and service providers from making available new services that are not wiretap capable. We believe that is inconsistent with basic human rights for a government to demand that no conversation should ever be free from being overheard. While we recognize that many telecommunications networks have the capability for interception, making it a primary function of the system changes the nature of the network and places a chill on free speech and other human rights.

This will also negatively affect the development of new technologies and efforts to provide access to telecommunications to all citizens in South Africa. In the United States,

the Communications Assistance for Law Enforcement Act (CALEA) has delayed the development of new telephone, cellular and satellite communications technologies as conflicts over the development and implementation of surveillance standards have continued. Similar problems have occurred in the Netherlands and Australia.

Article 7 also fails to include many of the important stakeholders in the creation of the document on technical surveillance standards. 7(4) authorizes the Minister to discuss the standards with Service Providers but not with independent technical experts, human rights groups and others with an interest in the implementation of the legislation. This closed process ensures that privacy interests will be sacrificed to real other goals.

The list of criteria in Article 7(5) is unbalanced and places the interests of surveillance over all others. It fails to include factors such as cost effectiveness and assurances that privacy and human rights will be protected by technical measures from unauthorized interceptions. In contrast, CALEA requires that any standards:

- (1) meet the assistance capability requirements ... by cost-effective methods;
- (2) protect the privacy and security of communications not authorized to be intercepted;
- (3) minimize the cost of such compliance on residential ratepayers;
- (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and
- (5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers during any transition period.

This bill will also likely cause more Internet security problems and crime. Internet security is a major concern and there are frequent reports that network security flaws are being exploited. By requiring these capabilities, the bill will cause the introduction of more security flaws into telecommunications networks. Any protocol that requires methods of ensuring surveillance will create new security holes that can be exploited. In addition, the increased complexity of the systems will further undermine security and increase costs of development and implementation. The U.S. National Research Council's 1999 "Trust in Cyberspace" report identified increasing complexity as a core cause of decreasing security. The new security holes will likely cause more economic and personal harm than any interceptions facilitated will prevent.

LEGAL STANDARDS FOR TRANSACTIONAL AND LOCATION INFORMATION

In Article 1, the bill defines “call-related information” very broadly to include a wide variety of information that is not considered content, including web traffic and mobile telephone location information. Under Article 9, this information can be obtained without requiring a court order at the written request of representatives of the police, military and intelligence services. The information can be routed to the government monitoring centers for real-time surveillance or in other forms. It is crucial for the protection of privacy and human rights that transactional data created by new technologies is given greater protection under law than traditional telephone calling records. We recommend that a court order be required due to the sensitivity of the information.

When surfing the net, a user can visit dozens of sites in just a few minutes and reveal a great deal about their personal situation and interests. This can include medical, financial, social interests and other highly personal information. The detailed and potentially sensitive nature of the data makes it more similar to content of communications than telephone records and it should be treated as content.

Even if the actual pages viewed are considered content and given greater legal protections, the transactional information still can reveal a great deal of information. For example in a standard visit to www.google.com, a search engine site, the content of that communication is the packets returned which consists of graphics and text; but this does not include the actual request to www.google.com, which would be:

[http://www.google.com/search?hl=en&q="Aids+treatment"&btnG=Google+Search](http://www.google.com/search?hl=en&q=)

which quickly becomes as invasive as the interception of content information for the purpose of investigations because it reveals the interests of the user and the details of the content they are reading.

The same concerns apply to the interception of email header information. While superficially this would appear analogous to the collection of telephone calling records, there are important differences which make the information more sensitive and thus requiring greater legal protections: 1) unlike the telephone system, which is a point to point system between two fixed devices that can be used by anyone with physical access, email is usually a person to person system; 2) email communications usually include a subject which gives an indication of the content; and 3) the size of the communication can also reveal the nature of the content (i.e. a media file or long text or a short answer).

The need for greater protection is recognized by many countries around the world. The European Union’s 1997 Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector requires that telecommunications providers delete signaling information once it is no longer for the communications. The Council of Europe’s working group on cyber-crime in their recent final report on the COE Cybercrime Convention, noted:

Some states consider the collection of traffic data as being equivalent to the collection of content data in terms of privacy and intrusiveness. The right of reservation would permit these states to limit the application of the measures to collect traffic data, in real-time, to the same range of offences to which it applies the powers and procedures of real-time interception of content data.

Location information generated by mobile communications is similarly sensitive and a court order should be required. Location information can provide details of an individuals' movements and activities and whom they have met with. This affects a wide variety of civil liberties protected by the SA Constitution beyond the right of privacy including the rights of free speech and assembly.

Finally, under this Article and under Article 11, there is no limitation set on the duration for which this information can be held. South Africa is still lacking a law protecting personal data as required by the Constitution and as was originally included in the Open Democracy Bill. We urge the Parliament to move forward on adopting that act.

COSTS

The bill requires that industry providers bear the costs of upgrading and maintaining their networks to make them wiretap capable. This will result in increased surveillance, a stifling of innovation, the reducing 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 privacy community has supported those requests.

Requiring that law enforcement 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 from many countries that law enforcement places unreasonable demands on providers for expansive surveillance capabilities without justifying their demands.

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. For many new technologies where innovative approaches are being developed, adding in capabilities can be quite difficult. While it is thought that a market for technologies with embedded surveillance capabilities may emerge and lessen the costs, there are three intertwined problems with this resolution. 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 closed standards bodies (ETSI for example with its Internet and mobile

telephony efforts); 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 facilitating more electronic surveillance.

Countries that have attempted to impose all of law enforcement's 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 the SA bill and 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 implement as there is little experience in creating such capabilities in networks. The industry organization of internet service providers in the Netherlands (NLIP) has estimated that the costs will range from half to 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 intercept 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, particularly with the lack of skilled workers available. 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 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 annual public reporting of information about 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 South African 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 about the number of uses of electronic surveillance, the types of crimes that they are authorized for, their duration and other information. In the U.S., 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 U.K., the Interception of Communications Commissioner publishes the report.

These countries recognize 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 the activities of law enforcement.

A number of countries including the United Kingdom and France also have special commissions that review wiretap usage and monitor for abuses. These bodies have expertise that most judges who authorize 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 oversight 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.

CONCLUSION

While we understand the importance of combating serious crime in South Africa, we believe that the lack of legal protections in this bill will invite abuse and have a severe impact on human rights and privacy. We recommend that substantial modifications be made before there is any further consideration of approving it.

We thank you for this opportunity to comment. If you have any questions, please feel free to contact David Banisar, deputy director at +1 202 483-1217 or by email at dbanisar@privacy.org.

Sincerely,

/sig

David Banisar
Deputy Director