SOUTH AFRICAN LAW COMMISSION

PROJECT 105

REVIEW OF SECURITY LEGISLATION

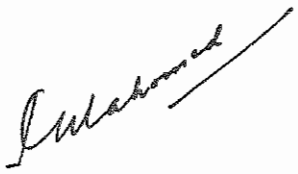
THE INTERCEPTION AND MONITORING PROHIBITION ACT
(ACT No. 127 OF 1992)

Report

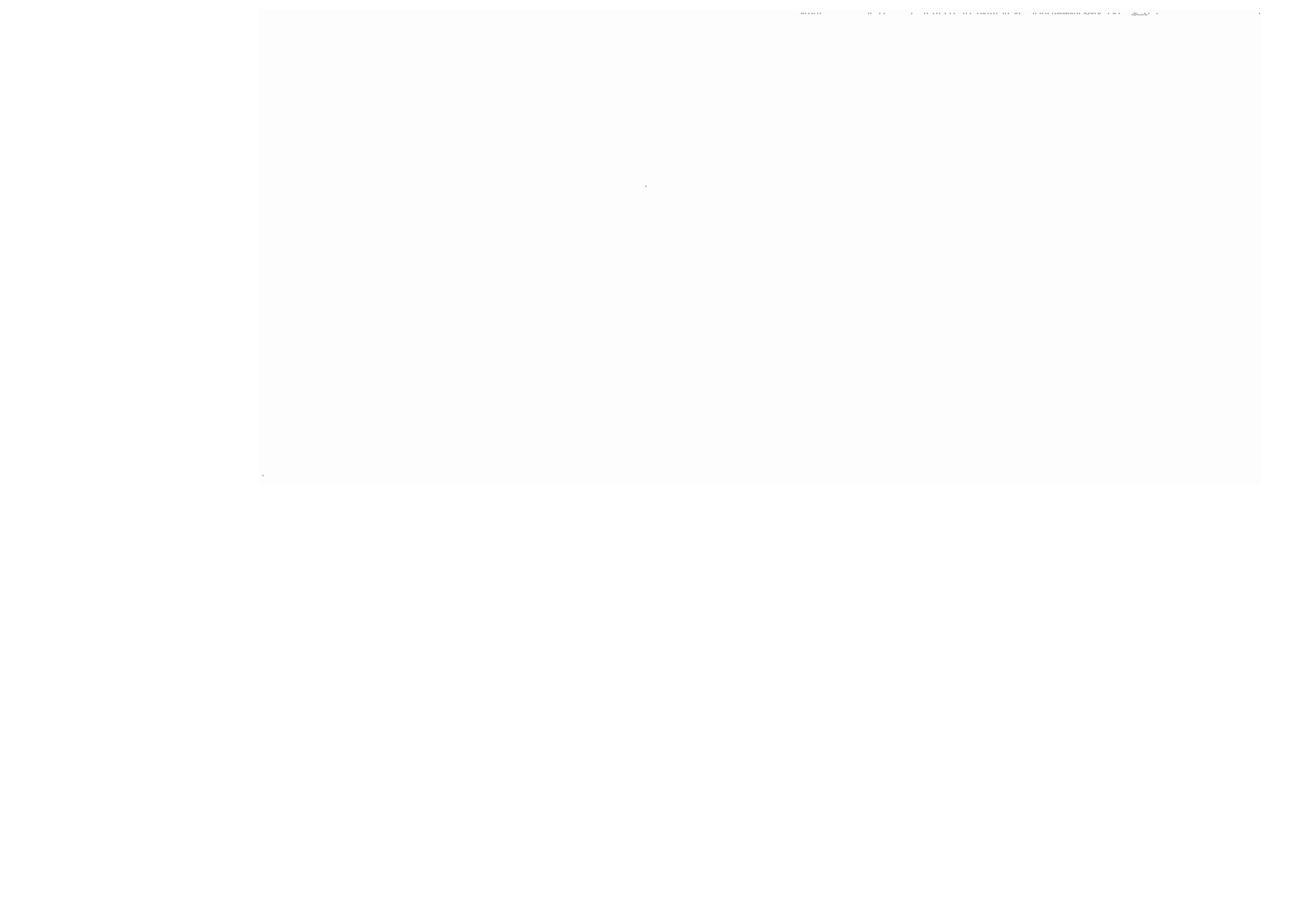
OCTOBER 1999

TO DR P MADUNA, MINISTER FOR JUSTICE AND CONSTITUTIONAL DEVELOPMENT

I am honoured to submit to you in terms of section 7(1) of the *South African Law Commission Act*, 1973 (Act 19 of 1973), for your consideration the Commission's report on The Interception and Monitoring Prohibition Act, 1992.



I MAHOMED
CHAIRPERSON: SA LAW COMMISSION
OCTOBER 1999



INDEX PAGE NO

SUMMARY OF RECOMMENDATIONS

The Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992), is reviewed in this report, with reference to, and in comparison with, the legal position in France, the Netherlands, Belgium, Germany, Britain, the United States of America, Hong Kong and Canada.

The working committee approved the publication of discussion paper 78 for general information and comment on 27 November 1998. The discussion paper contained provisional recommendations and a draft Bill. Twenty seven respondents commented in writing on the discussion paper. The project committee met on 29 May 1999 with parties representing telecommunication service providers, law enforcement, intelligence and security agencies. Their views and those reflected in the written comments were taken into account when the project committee considered its recommendations. The project committee's recommendations were considered by the Commission on 13 August 1999 and 22 October 1999. This report represents the Commission's final views on the Interception and Monitoring Prohibition Amendment Bill (see the proposed Bill contained in Annexure A).

The Commission makes the following recommendations in regard to amending the Interception and Monitoring Prohibition Act, 1992, namely-

1. that a definition of call-related information be inserted into the Act in order to define what call-related information is, namely "'call-related information' includes switching, dialling or signalling information that identifies the origin, destination, termination, duration and equipment identification of each communication generated or received by a customer or user of any equipment, facility or service rendered by a person, body or organization rendering a telecommunication service, and where applicable the location of such user at the time of the initiation or first reception of a call". (See paragraphs 12.2.1.21 - 12.2.1.26);
2. that a definition of communication be inserted into the Act in order to define what is meant by the term. (The Commission notes that the Act was amended as recently as 1998 by the insertion of the phrase "or conversations" in the definitions of "monitor"and "monitoring device" and in sections 2(1)(b) and (c) and 5(1)(a) and the phrase "conversation or" into section 4(2)(a) to make it clear, as the SAPS pointed out, to ensure that all types of communications, namely fax, e-mail, etc. may be intercepted

and the obligation be created in regard to telecommunication service providers to assist in executing directions in respect of not only *"conversations"* but also *"communications"*. The Commission is of the view that this aspect could be made much clearer if the Act were to include a definition on "communication" which provides that "communication" includes conversation and a message, and any part of a conversation or message, whether in the form of speech, music or other sounds, data, text, visual images, whether or not animated or signals, or in any other form or in any combination of forms. The Commission further recommends that, as a consequence of the definition of communication which includes conversations, references to "conversations" be deleted throughout the Act.) (See paragraphs 12.2.4.4, 12.2.4.13 and 12.2.4.15);

3. that the definition of a judge be further defined by substituting the term High Court for the term Supreme Court and to delete the reference to a particular division in regard to a retired judge who is designated by the Minister to perform the functions of a judge; (See paragraph 12.2.2.5);

4. that further provision be made in the definition of "serious offence" for offences to fall within the ambit of the Act ie to include other compelling national interests of the Republic (in addition to offences which may allegedly harm the economy and which are presently included as serious offences); any offence referred to in sections 13(f) and 14(b) of the Drugs and Drug Trafficking Act, 1992; any offence relating to the trafficking in firearms, ammunition and explosives; any offence relating to the death or serious bodily harm of any person; any offence referred to in the Prevention of Organized Crime Act of 1998; and any offence threatening the security of the Republic. (The Commission initially considered that provision ought to be made in the Bill for the offences contemplated in sections 100 and 101 of the Telecommunications Act 103 of 1996 to be serious offences for purposes of the Interception and Monitoring Prohibition Act. This would mean that the South African Telecommunications Regulatory Authority (SATRA) would be able to lay a charge with and request the SA Police Service to apply for a directive to authorise the interception and monitoring of telecommunications once SATRA inspectors have reasonable grounds to believe that telecommunication service providers are in breach of the provisions of the Telecommunications Act. The Commission however on reflection does not consider that such a provision would be appropriate in the light of the offences under discussion. The Commission further considers that the category of bodies who are presently empowered to apply for directives under the Interception Act, namely the SA Police Service, the National

Defence Force, the Secret Service and the National Intelligence Agency should not be expanded to include the South African Telecommunications Regulatory Authority too. The Commission also considers that the existing proviso setting out that the offence concerned is being or has been committed over a lengthy period of time should be deleted.) (See paragraphs 12.2.3.24 - 12.2.3.26 and 12.2.32.1 - 12.2.32.4);

5. that the definition of "telecommunications line" be substituted in the Bill with "telecommunications system" as defined in the Telecommunications Act; (See paragraphs 12.2.1.17, 12.2.1.25 and 26);

6. that the definition of "telecommunication service" be inserted into the Act setting out that it means any telecommunication service as defined in the Telecommunications Act, 1996; (See paragraphs 12.2.4.11, 12.2.4.12 and 12.2.4.14);

7. that it be made further clear that members of the South African Police Service, the South African National Defence Force, the Agency and the Service may only intercept or monitor communications if a directive is issued by a judge in terms of the Act to authorise such interception or monitoring. (The Commission considers that the reasoning by Judge Cameron in the *Kidson* case is persuasive and that where police, defence and intelligence agency personnel wish to monitor communications for the purpose the statute specifies, they must in terms of sections 2(2) and 3 obtain authorisation even for participant monitoring.) (See paragraphs 12.2.5.22 - 12.2.5.36);

8. that further provision be made for the designation of judges considering applications under the Act, provided that the Minister may designate a judge for more than one division. (The provisional recommendation was that provision should be made for the designation of particular judges considering applications relating to state security only, and that judges be designated particularly to consider applications relating to serious offences. The Commission is of the view that there is so much overlapping of matters involving serious crimes and state security that it would be inadvisable to try to separate them. Presently a direction may only be considered by the judge designated for the division from where the postal article or communication has been or will probably be dispatched or transmitted or where that postal article or communication will probably be received.) (See paragraphs 12.2.6.16 - 12.2.6.19);

9. that section 3(1)(b) be amended to provide that the judge concerned may issue a directive if he or she is satisfied on the facts alleged in a written application that there are reasonable grounds to believe that a serious offence has been or is being committed or will be committed and that the offence cannot be investigated in another

appropriate manner. The Commission further recommends that section 3(b)(ii) be amended by the insertion of the phrase "interests" in order to provide "that the security or compelling national interests of the Republic are threatened or that the gathering of information concerning a threat to the security or compelling national interests of the Republic is necessary". (The Act provides presently that a judge may issue a directive if convinced that the offence that has been or is being committed or will probably be committed, is a serious offence that cannot be properly investigated in any other manner or that the security of the Republic is being threatened or that the gathering of information concerning a threat to the security of the Republic is necessary.) (See paragraphs 12.2.7.11 - 12.2.7.17);

10. that a clause 3(7) be inserted in the Act making provision that no communication between a legal representative and his or her client may be intercepted or monitored, except if on reasonable grounds, the judge is satisfied that such a legal representative is involved in, or aiding or abetting a serious offence or an offence threatening the security of the Republic. The Commission considers that there is a need to regulate attorney/client privilege in the Act and that the same standard of assessment should apply in this clause as is proposed in section 3(1). (See paragraphs 12.2.8.7 - 12.2.8.9);

11. that a clause 3(8) be inserted into the Bill setting out that the judge may upon application direct further additions or amendments to an existing directive if he or she is satisfied that the addition or amendment is necessary. (The Commission notes that where there is a need for an existing directive to be altered then it should not be necessary to bring a fresh application for a directive to be issued. The Commission is of the view that this is a sensible addition, that it would permit an application to a judge who was originally seized with the matter and that it makes sense that the Act should make provision for such additions or variations of existing directives.) (See paragraphs 12.2.7.15 - 12.2.7.17);

12. that there is no need to make provision for persons or bodies other than the SA Police Service, the National Defence Force, the Secret Service and the National Intelligence Agency to make applications under the Act. (It was suggested that the Office of President ought to be vested with a right to make an application for the interception and monitoring of all State Departments within the confines of the Act and that registered, qualified or listed private investigators likewise be vested with such a right to make applications. The Commission is not persuaded by this proposal. The Commission

considers that the position should remain as set out in the Act, which entitles only the SA Police Service, the National Defence Force, the Secret Service and the National Intelligence Agency to make applications under the Act.) (See paragraphs 12.2.34.2 - 12.2.34.5);

13. that a clause 5(4) be inserted in the Act making provision that the remuneration referred to in sections 5(2) and (3) shall only be in respect of direct costs incurred in respect of personnel and administration and the lease of telecommunications systems, where applicable, and shall not include the costs of acquiring the facilities and devices referred to section 5A(2). (The Commission notes that there are presently negotiations being conducted involving, inter alia, the law enforcement and intelligence agencies and the cellular telecommunication operators. The Commission further notes that a legitimate debate is conducted as to where the costs should lie in regard to the financial implications which will result from the proposed amendments, should they be effected. The Commission takes into account that on the one hand, the present cellular operators and Telkom take the attitude that they pay their taxes and that the revenue derived from these taxes, should be appropriately directed. The Commission was advised by these parties that law enforcement, of which the Interception and Monitoring Prohibition Act is a part, is quintessentially a function of the State. The Commission also notes the opposing view that telecommunications operators are in possession of a very productive and lucrative resource, and that it is therefore appropriate in those circumstances that they should bear particular obligations. Having further regard to modern technology and criminal methods, including the use of their products, the Commission considers that it is entirely appropriate that the telecommunication operators should bear the costs as is proposed in the Amendment Bill. The Commission is of the view that this is an indeterminable debate which will not be resolved by it.) (See paragraphs 12.2.9.16 - 12.2.9.19);

14. that a clause 5A(1) be inserted in the Act and provision be made in the Act that no person, body or organization rendering a telecommunication service, may provide any such service which does not have the capacity to be monitored. (The Commission is of the view that use should be made in clause 5A(1) of the term "capacity" and not "capability". The Commission is further of the view that the concerns of respondents on the issue of encryption should be dealt with in the suggested provision. The Commission considers that the provision should make it clear that a service provider will not be responsible to decrypt any encrypted communication unless the facility for

encryption forms part of the service rendered by the service provider.) (See paragraphs 12.2.10.19 - 12.2.10.23);

15. that a clause 5A(2) be inserted in the Act and provision be made that any person, body or organization rendering a telecommunication service shall at own cost and within the period specified in a directive by the Minister for Posts, Telecommunications and Broadcasting, acquire the necessary facilities and devices to enable the monitoring of conversations and communications. (The Commission notes that the costs issue is at the heart of the matter but notes that this aspect is presently being negotiated. The Commission also notes the concerns of the telecommunication service providers being prescribed from which suppliers they should acquire the devices and facilities necessary to enable monitoring. In the Bill contained in the discussion paper it was proposed that the telecommunication service providers should acquire the devices and facilities concerned from a supplier approved by the Minister for Posts, Telecommunications and Broadcasting. The Commission is of the view that it does not matter what equipment the service providers acquire, provided it has the capacity to intercept and monitor.) (See paragraphs 12.2.11.14 - 12.2.11.16)

16. that a clause 5A(3) be inserted in the Act and that provision be made that the investment, technical, maintenance and operating costs in enabling a telecommunication service to be monitored, shall be carried by the person, body or organization rendering such a service; (See paragraphs 12.2.12.6 - 12.2.12.8);

17. that a clause 5A(4) be inserted into the Act and provision be made that duplicate signals of conversations and communications authorized to be monitored in terms of the Act, shall be routed by the relevant person, body or organization rendering a telecommunication service to the relevant central monitoring centre, to be designated by, respectively, the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force, and the Directors-General of the Agency and Service; (See paragraphs 12.2.13.3 - 12.2.13.4);

18. that a clause 5A(5) be inserted in the Act and provision be made that the South African Police Service, the South African National Defence Force, the Agency and the Service shall, at State expense, equip, operate and maintain central monitoring centres for the authorized monitoring of conversations or communications: Provided that an agreement on the sharing of any such central monitoring centre shall not be excluded. (See paragraphs 12.2.14.2 - 12.2.14.3);

19. that a clause 5A(6) be inserted in the Act and provision be made that the Minister for

Posts, Telecommunications and Broadcasting after consultation with any person, body or organization rendering a telecommunication service, may issue a directive to comply with the provision on the rendering of services which are capable of being monitored and that he or she may specify the security, technical and functional requirements of the facilities and devices to be acquired in terms of subsection (2). (See paragraphs 12.2.15.5 - 12.2.15.7) ;

20. that a clause 5A(7) be inserted in the Act and to make provision for the particular specifications set out in the directive issued by the Minister which he or she may require telecommunication service providers to comply with. (The Commission is of the view that the proposed clause is appropriate, particularly in view of the obligation on the Minister to consult with the relevant parties.) (See paragraphs 12.2.16.4 - 12.2.16.5);

21. that a clause 5A(8) be inserted in the Act and that provision be made that the Minister for Posts, Telecommunications and Broadcasting may, after consultation with the person, body or organisation rendering the telecommunication service, determine a period, which shall not be less than three months from the date on which a direction in terms of subsection (6) is issued, for compliance with such a directive. (See paragraphs 12.2.17.3 - 12.2.17.5);

22. that a clause 5B(1) be inserted in the Act making provision that any person who is authorised to apply for a directive in terms of section 2(2), may also apply, in the manner prescribed in this Act, for a supplementary directive for the provision on an ongoing basis for a specific duration of call-related information, as it becomes available. (See paragraphs 12.2.18.4 - 12.2.18.7);

23. that a clause 5B(2) be inserted in the Act making provision that any person, body or organization rendering a telecommunication service shall, in respect of all communications which are monitored in terms of this Act, route the call-related information specified in a supplementary directive to the relevant designated central monitoring centre. (See paragraphs 12.2.18.6 and 12.2.18.8);

24. that a clause 5B(3) be inserted in the Act making provision that, if in a specific case, only call-related information is required on an ongoing basis without the actual monitoring of the communication in question, the judge may direct that the relevant person, body or organisation rendering a telecommunication service to whom or which a directive is addressed, provide such call-related information to the South African Police Service, the South African National Defence Force, the Agency or the Service, whichever is applicable. (See paragraphs 12.2.19.5 - 12.2.19.7);

25. that a clause 5B(4) be inserted in the Act making provision that the availability of the procedures set out in the Bill in respect of the ongoing provisioning of call-related information excludes the use of any power in any other Act, to obtain evidence or information in respect of a person, body or organization. (The Commission notes that section 205 of the Criminal Procedure Act and section 11(1)(e) of the Drugs and Drug Trafficking Act, 1992 confers powers on law enforcement agencies to obtain evidence such as call-related information. The Commission poses the question whether this situation should be sanctioned by the proposed clause 5B(4) and whether the Interception Act should permit agencies to request the provision of call-related information. The question as to abuse of the provisions arises. The need for the existence of different methods of enabling law enforcement agencies to obtain call-related information seems questionable. The Commission is therefore of the view that the Interception and Monitoring Prohibition Act should be the only Act to authorise the request for call-related information and should exclude the use of any power in any other Act, to obtain evidence or information in respect of a person, body or organization. (See paragraphs 12.2.20.1 - 12.2.20.6);

26. that a clause 5B(5) be inserted in the Act making provision that any person, body or organization rendering a telecommunication service shall ensure that proper records regarding identities and addresses are kept in respect of clients to whom a telecommunication service is provided, whether on a prepaid or contract basis and to require positive identification from a client to whom such a service is provided. (See paragraphs 12.2.21.9 - 12.2.21.12);

27. that a clause 5B(6) be inserted in the Act making provision that any person, body or organization rendering a telecommunication service, shall provide such information regarding the customer who has contracted for the use of such telecommunication service to the South African Police Service, the South African National Defence Force, the Agency or the Service, as may be required by an officer or member, to fulfil the functions and exercise the powers authorized by law. (See paragraphs 12.2.22.7 - 12.2.22.8);

28. that a clause 5B(7) be inserted in the Act making provision for the provision of the name, identity number and address of the person contracted for the use of the telecommunication service. (See paragraphs 12.2.23.1 - 12.2.23.3);

29. that a clause 6(2) be inserted in the Act to provide that if a judge considers any case to be sufficiently urgent, the procedure set out in the Act may be dispensed with and the

matter may be dealt with in such manner and subject to such conditions as the judge may deem fit, including the grant in any appropriate case of an oral directive followed up by written application incorporating the terms of the directive within one week, and that where an oral directive was issued, the judge must reduce it to writing within two days. (See paragraphs 12.2 24.12 - 12.2.24.15);

30. that a clause 6A(1) be included in the Act making provision that the use of any information obtained through the application of the Act, or any similar Act in another country, as evidence in any prosecution, is subject to the decision of a Director of Public Prosecutions or an Investigating Director. (The Commission considers that although the Directors of Public Prosecutions may already have the power to lay down guidelines on which evidence may or should be presented to court, as the project committee pointed out, it is appropriate to set these powers out in the Interception and Monitoring Prohibition Act. The Commission is therefore in favour of the inclusion of the clause.) (See paragraphs 12.2.25.4 - 12.2.25.7);

31. that a clause 6A(2) be inserted in the Act making provision that information regarding the commission of any criminal offence, obtained by means of any interception or monitoring in terms of the Act, or any similar Act in another country may be admissible as evidence in criminal proceedings. (The Commission is of the view that although it might be correct to assert that the clause does not add anything new, as the project committee argued, legal certainty could be effected if the Bill were to set out what the consequences are if evidence is obtained as a result of a directive requested regarding the commission of a certain criminal offence, and information is obtained regarding the commission of any other serious offence.) (See paragraphs 12.2.26.12 - 12.2.26.15);

32. that a clause 8(1A) be inserted in the Act making provision that any person, body or organization rendering a telecommunication service and failing to comply with a directive issued by a judge, a directive issued by the Minister for Posts, Telecommunications and Broadcasting, the obligation to provide information regarding a customer contracted for the use of a telecommunication service, the obligation to keep records, or the obligation to require positive identification when contracting a telecommunication service shall be guilty of an offence, and liable on conviction, to a maximum fine of R 200 000. The Commission considers that the proposed maximum fine is not excessive or inappropriate.) (See paragraphs 12.2.27.8 - 12.2.27.10);

33. that a clause 8A be inserted in the Act making provision that if any person, body or organization rendering a telecommunication service, fails, after a conviction for failing

to comply with a directive, to comply with a further such directive, the Minister for Posts, Telecommunications and Broadcasting may revoke the licence issued in terms of Chapter V of the Telecommunications Act, 1996, to such person, body or organization to render a telecommunication service.) (See paragraphs 12.2.28.3 - 12.2.28.5);

34. that no provisions seeking to regulate the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices be included in the Bill. (Respondents were invited to advise the Commission on their views regarding measures to regulate the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices. The Commission noted in particular the comments by the office of the Deputy Minister of Intelligence which stated that this issue should be part of new legislation and not as part of the Monitoring and Interception Prohibition Act, 1992, arguing that it is not the appropriate legislation to deal with these issues, that the matter has policy implications, which require further discussion with the Security Ministers and the Joint Standing Committee on Intelligence and that any new ideas on the matter will be addressed before legislation is taken to Parliament. The Commission therefore recommends that this aspect be dealt with in separate legislation.) (See paragraphs 12.2.29.14 - 12.2.29.15);

35. that there is no need to include detailed provisions in the Bill regulating how interceptions of communications should be recorded, sealed and stored in order to overcome all potential evidential concerns. (One assertion by respondents is that the statute under discussion is detailed enough, that exhaustive detail can have its disadvantages and result in endless litigation, whereas the opposing assertion is that since fundamental rights are encroached upon by this legislation, strict and detailed procedures should be laid down in the Act. A detailed procedure similar to American legislation prescribing the method for taping interceptions was advocated. The Commission is of the view that it seems questionable whether the existing US provisions will solve all evidential problems concerning recordings.) (See paragraphs 12.2.30.5 - 12.2.30.7);

36. that the matter of hacking and the broader issue of the desirability of legislation governing the Internet such as an Internet Communications Act be dealt with in the Commission's investigation into computer related crimes (project 108) and not in this investigation. (See paragraphs 12.2.31.1 - 12.2.31.2);

37. that section 4 of the Act be amended to provide that any other person which has been authorized thereto, may execute or assist in the execution of a direction. (The Act

presently provides that any member of the Force as defined in section 1 of the South African Police Service Act, 1995 or a member, excluding a member of a visiting force, as defined in section 1 of the Defence Act, 1957 or a member of the Agency or the Service may execute a direction, provided that the member concerned has been authorized by the officer or member who made the application in terms of section 3 (2) to execute that direction or to assist with the execution of the direction. The SAPS notes that it has various civilian personnel who is not per definition a member as defined in section 1 of the South African Police Service Act, 1995, but who could, for instance, assist in the transcription of tapes.) (See paragraph 12.2.33.1 - 12.2.33.2);

38. that no provision be made in the Bill for telecommunication service providers being permitted to answer directives by way of affidavit (It was suggested that due to the sensitive nature of the information, MTN be allowed to answer the directives by way of affidavit, and that to protect its employees a structure should be created in the event of any judicial proceeding whereby the aforementioned affidavit will be used in such proceedings and MTN employees will not be required to testify in Court. The Commission is of the view that there is no need to confer the proposed power to officials employed by telecommunication service providers.) (See paragraphs 12.2.35.1 - 12.2.35.3);

39. that the Bill make provision that any person who intercepts or monitors a conversation or communication in accordance with a directive issued under the Act or who in good faith assists a person who he or she believes on reasonable grounds is acting in accordance with a directive, is not guilty of an offence. (It was suggested that MTN and any licenced telecommunications operator be indemnified from any claims where MTN acted in accordance with a *prima facie* written directive.) (See paragraph 12.2 36.1 - 12.2.36.2);

40. that no provision need to be made in the Bill for directives being served upon telecommunication service providers at certain central points. (MTN submitted its preference to written directives being served upon MTN at a central point in order for effect to be given to the purport of this particular Bill.) (See paragraph 12.2.37.1 - 12.2.37.2).

BIBLIOGRAPHY

LIST OF CASES

A v France Application No 14838/89 (European Court of Human Rights) .

Halford v United Kingdom (1997) 3B HRC 3 (European Court of Human Rights).

Klass and Others: Judgment of the European Court of Human Rights: Strasbourg 6 September 1978.

Lambert v France Application No 88/1997/872/1084 (European Court of Human Rights)

Malone case European Court of Human Rights (4/1983/60/94) Strasbourg 2 August 1984.

Protea Technology Ltd and Another v Wainer and Others (1997) 3 All SA 594.

R v Broyles [1991] 3 SCR 595.

R v Duarte [1990]1 SCR 30.

R v Wong [1990] 3 SCR 36.

S v Kidson 1999 (1) SACR 338 (W).

S v Naidoo and Another (1998) 1 All SA 189.

S v Nkabinde and Another Case No. CC124/97 Pietermaritzburg High Court.

LEGISLATION

Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992) (South Africa)

Interpretation Act, 1957 (Act No. 33 of 1957) (South Africa)

Criminal Procedure Act, 1977 (Act No. 57 of 1977) (South Africa)

Loi no 9 - 646 du 10 Juillet 1991 *relative an secret des correspondances émises por la vioce des telecommunications* (France)

Telecommunications Bill, 1998 (Netherlands)

Wet van 30 Junie 1994 - *ter bescherming van de persoonlijke levensfeer tegen het afluisteren, kennisnemen en openen van privécommunicatie en telecommunicatie* (Belgium)

Interception of Telecommunications Act, 1985 (Britain)

Foreign Intelligence Surveillance Act (FISA) (United States of America)

Omnibus Crime Control and Safe Streets Act (18 USC Title III) United States of America

Communications Assistance for Law Enforcement Act (CALEA) Public Law 103 - 414; 47 USC 1001 - 1010. (United States of America)

Criminal Code Part VI Canada (Invasion of privacy)

Electronic Communications Privacy Act 1986 (United States of America)

SOURCES CONSULTED

Beeld 1998-04-23 "Nkabinde - regter verstom oor afluistering".

Burke "Secret Surveillance and the European Convention on Human Rights" 1981 *Stanford Law Review*, p 1113 - 1140

Chappell Dr Duncan "Law Enforcement Co-operation: The Interception of Communications and the Right to Privacy" Paper presented at the Oxford Conference on International Co-operation in Criminal Matters: Balancing the protection of human rights with the needs of law enforcement 24 - 28 August 1998, Christ Church, Oxford, UK

Carr James G *The Law of Electronic Surveillance* Clark Boardman Company: Ltd New York 1986.

Carr James G "Wiretapping in West Germany" 1981 *American Journal for Comparative Law* p 607 - 645.

Commission of Enquiry Concerning certain Activities of the Royal Canadian Mounted Police second report *Freedom and Security under the Law* August 1981.

Commission Nationale de Contrôle des Interceptions de Securité *Report for 1997* La Documentation Francaise, Paris 1998.

Clark M Wesley "Electronic Surveillance and Related Investigative Techniques" 1990 *Military Law Review* Vol 128 p 155.

Cramer Vicky "Cellular phones: Walking the tightrope between technology and security" 4 April 1998 *Security Focus* Vol 11 p 6.

Cramer Vicky &Van den Hout, PJ *Het afluisteren van telefoongesprekke als dwangmiddel.* Gouda Quist/Noordwijl: Kluwer 1989.

Crawford Kimberley A "Surreptitious Recording of Suspect's Conversations" September 1993 *FBI Law Enforcement Bulletin* p 26.

Editorial "Hou die Regbank ongeskonde" October 1992 *Consultus.*

Denning Dorothy E Denning "To tap" *Georgetown University Comm of the ACM* March 1993 Vol 36 No 3 p 24.

European Union *Internationale Anforderungen für die rechtmässige Überwachung des Telekommunikationsverkehrs* January 1995.

Fishman Clifford S "Interception of communications in exigient circumstances: the Fourth Amendment, Federal Legislation, and the United States Department of Justice" Fall 1987 *Georgia Law Review* Vol 22 No 1 p 1.

Fishman, Clifford S *Wiretapping and Eavesdropping* New York: The Lawyers Co-operative Publishing Co. 1978.

Fijnaut Cyrille Marx Gary T *Undercover Police Surveillance in Comparative Perspective* Boston: Kluwer Law and Taxation Publishers 1995

Federal Bureau for Investigation *Federal Register* Oct 16 1995 (vol 60) No 199 Notices. Page 53643-53646 from Federal Register Online via GPO access. Initial notice and request for comments. CALEA.

General Secretariat: International Telecommunications Union. *International Telecommunication Convention, Final Protocol. Additional Protocols, Optional Additional Protocol,Recommendations and Opinions* Nairobi, 1982.

Global Crime Update No 18 - May 29 1998.

Goldstein "The Eavesdropping Law" 1980 *Israel Law Review* vol 15 p 144-153.

Hecht Jonathan "Internal Security: Establishment of a Canadian Security Intelligence Service" 1985 *Harvard International Law Journal* p 234-349.

Hunt PMA *South African Criminal Law and Procedure* Kenwyn: Juta and Co Ltd 1990.

1995 Illinois Criminal and Traffic Law Manual. Gould Publishers.

Kresse John R "Privacy of Communications over Cordless and Cellular Telephones: Federal Protection under the Electronic Communications Privacy Act of 1986" 1987 *George Mason University Law Review* vol 912 p 335-350.

Law Refrom Commission of Canada *Report No 33 Recodifying Criminal Procedure* Volume One Title I

Lensing JAW *Criminal Law* The Hague: Kluwer Law International 1997.

Long Colin D *Telecommunications Law and Practice* London: Sweet and Maxwell 1988

Marshall Harold "Fax machine cannot be bugged like a telephone" March 1992 *Security Focus* p 77.

Mathews Anthony S *Freedom, State Security and The Rule of Law Kenwyn:* Juta and Co Ltd 1986.

Ploman Edward W *International Law Governing Communications and Information* London: Frances Pinter (Publishers) Ltd. 1982.

Report: Commissioner for 1990 *Interception of Communications Act, 1985* April 1991.

Report of the Committee of Privy Councillors appointed to inquire into the Interception of Communications London: Her Majesty's Stationery Office. October 1957 Cmnd 283.

Roos Annelise "Nuwe telekommunikasie tegnologie lei tot vrese vir privaatheidskending in die Verenigde State van Amerika" Oktober 1991 *Codicillus* Vol XXXII No 2 p 19.

Ruiz Blanca R *Privacy in Telecommunications* The Hague: Kluwer Law International 1997.

Snyman CR *Strafreg* Durban: Butterworths 1992.

South African Law Commission *Interim Report: Group and Human Rights* Project 58 Pretoria: SA Government Printer August 1991.

Standing Committee on Law and National Security FISA Court Chief Judge Royce Lamberth discusses Work of Courts *National Security Law* Report Vol 19 No 2 May 1997.

The Citizen 1998-03-04 "Counsel challenges validity of tape" p 9 .

The Citizen 1997-09-22 "Clinton's pager traffic intercepted by hacker".

The Citizen 1997-03-13 "Fined for bugging wife's phone calls".

The Law Reform Commission of Hong Kong *Consultation paper on Privacy: Regulating surveillance and the Interception of Communications* June 1996.

The Law Reform Commission of Ireland *Report on Privacy: Surveillance and the Interception of Communications* LRC 57 - 1998 June 1998.

The 1996 Annotated Tremeear's Criminal Code by D Watt and M Fuerst Ontario: Carswell 1996

Van Niekerk B v D "Unbugging the bug, or the right to be left alone in Criminal Law: Some Reflections" 1971 South African Law Journal p 171.

Wagner André "Bugging - the invisible threat" January 1995 *Security Focus*

Weekly Mail 11 - 17 June 1993 "Burger grilled in bugging trial" p 4.

Yost Graham *Spy Tech Telephone surveillance and counter-surveillance* Chapter 4 p 164 - 230.

CHAPTER 1

A. ORIGIN OF THE INVESTIGATION

1.1 In November 1995 the Commission considered a request from the Minister for Safety and Security that a review and rationalisation of South Africa's security legislation should be undertaken by the Commission.[1] The Minister for Safety and Security suggested that in view of the history of security legislation and changed circumstances in South Africa, all existing legislation such as the Internal Security Act, 1982, should be enacted in accordance with international norms, the Constitution and the country's present circumstances and requirements.

1.2 The then Chairperson of the Commission, Mr Justice H J P van Heerden, informed the Minister that the Commission was willing to undertake a review of security legislation and he requested logistical support from the Department of Safety and Security or the Department of Justice. The Chairperson also suggested the establishment of a project committee of experts to advise the Commission and to consider the papers drafted during the course of the investigation.

1.3 At its meeting on 23 and 24 February 1996, the reconstituted Commission endorsed both the views expressed by its predecessors in this regard and the establishment of a project committee composed of suitably qualified experts. The Minister of Justice was subsequently requested to approve the inclusion of the investigation in the Commission's programme. On 22 March 1996 he approved the inclusion of the investigation on the Commission's programme. The Commission designated Madam Justice Mokgoro, being one of its Commissioners, to serve on the project committee. On 1 October 1998 the Minister of Justice appointed the following persons to serve on the project committee on security legislation:

- Mr Justice CT Howie of the Supreme Court of Appeal in Bloemfontein;
- Ms P Jana, a Member of Parliament;
- Mr GJ Marcus SC an advocate at the Johannesburg Bar;
- Mr D Nkadimeng, an attorney from Pietersburg; and

---

1 Addressed to the Minister of Justice which the Minister of Justice referred to the Commission.

- Mr D Tabata, an attorney from King William's Town.

1.4 In the meantime, Parliament has adopted the Safety Matters Rationalization Act, 1996 (Act No. 90 of 1996), which repealed a number of South African Acts dealing with security legislation, including those of the former TBVC states, which was clearly inconsonant with the interim Constitution.[2] A total number of 34 laws were repealed in the process, whilst the operation of the following Acts of the Republic of South Africa was extended to the whole national territory of the Republic :

* The Riotous Assemblies Act, 1956 (Act No. 17 of 1956);
* The Explosives Act, 1956 (Act No. 26 of 1956);
* The Intimidation Act, 1982 (Act No. 72 of 1982);
* The Internal Security Act, 1982 (Act No. 74 of 1982) (as amended by section 1 of the Safety Matters Rationalization Act, 1996);
* The Demonstrations in or near Court Buildings Prohibition Act, 1982 (Act No. 71 of 1982);
* The Regulation of Gatherings Act, 1993 (Act No. 205 of 1993).

1.5 The only provisions of the Internal Security Act, 1982, which remained in force are sections 54(1) and (2), and section 46(3), ie the offences of terrorism and sabotage and the power of the Minister for Safety and Security to prohibit gatherings in certain circumstances.

1.6 The Regulation of Gatherings Act, 1993, which repealed the Demonstrations in or near Court Buildings Prohibition Act, 1982, has been put into operation.

1.7 In this investigation the Law Commission will concentrate on matters such as :

* The review of the crimes of terrorism and sabotage - in order that South Africa can ensure that obligations in respect of international terrorism are fulfilled.
* The protection of classified information in the possession of the State.

---

2 It should be noted that there are also other Acts which deal with security matters such as the Protection of Information Act, 84 of 1982, the National Key Points Act, 102 of 1980, and the Defence Act, 44 of 1957. Hence, the list of Acts repealed is not inclusive of all the Acts which may be inconsonant with the Constitution.

* Interception and monitoring - the review of the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1992).
* Regulation of Private Intelligence Companies.
* Economic espionage as a threat to national security.
* Protection of the property and personnel of foreign governments and international organisations, including protection from intimidation, obstruction, coercion and acts of violence committed against foreign dignitaries, foreign officials and their family members.
* Hostage taking in order to compel any government to do or abstain from doing any act.

1.8 The Project Committee has decided to prioritize this investigation. It has been decided that the area which needs priority attention, is that of interception and monitoring of communications for crime investigation and intelligence gathering. The Project Committee will continue to prepare discussion papers on the other topics as its investigation progresses.

B. The consultative process

1.9 The Project Committee had its first meeting on 17 November 1998 and considered a draft discussion paper which was subsequently considered by the Working Committee of the Commission. The Working Committee approved the publication of discussion paper 78 which contained provisional recommendations and a draft Bill (which is enclosed in this report as Annexure C) for general information and comment on 27 November 1998. The availability of the discussion paper was announced at a media conference hosted at the Commission's offices on 14 December 1998, on the Commission's Website[3], in a Bulletin issued by the Commission dated 2 December 1998[4] and in the Government Gazette. The media also reported on the Commission's investigation and the provisional recommendations contained in the discussion paper.[5]

---

3 See http://www.law.wits.ac.za/salc/discussn/discussn.html

4 See http://www.law.wits.ac.za/salc/bulletin/bull3_2.html

5 See "Service providers face bill for bugging" *The Star* 15 December 1998 on 3 and "Commission proposes bugging law changes: Greater powers for judges" *The Citizen* 15 December 1998 on 5.

1.10 The discussion paper was distributed to approximately 400 local parties and bodies and to 250 foreign parties and bodies. Written comments were received from 28 respondents (see Annexure D).

1.11 Attempts were made for the consideration of the Interception and Monitoring Prohibition Amendment Bill by parliament earlier this year. Representatives of the cellphone industry requested the Minister of Justice that they be afforded further opportunity to make submissions before the legislation was considered in parliament. It was then decided that the Bill should not be further promoted in parliament and that the Commission should finalise the investigation. Representatives of Telkom, MTN, Vodacom, SATRA and the Police, Secret Service and National Intelligence Agency met with the project committee on 29 May 1999. The project committee then considered and amended the draft Bill taking into account the written submissions received and the oral submissions made during the meeting held on 29 May 1999.

1.12 The Commission considered the report and the draft Bill (see Annexure A) on 13 August 1999 and 22 October 1999. The submission of the report to the Minister was approved at the latter meeting.

C. Background

1.13 The Interception and Monitoring Prohibition Act, 1992, was put into operation on 1 February 1993. It was drafted before the adoption of the Interim Constitution, but at a time when the debate on a new constitutional dispensation and a Bill of Rights had already started. The Act was drafted without the framework of a democratic constitution, but with the knowledge that the Act will have to withstand the challenges of a constitutional state comparable to strict standards. At the time of drafting the Interception and Monitoring Prohibition Act, 1992, the South African Law Commission had already published a draft Bill of Rights for comments. Until recently, there was no provision in the territories of the previous TBVC states regarding interception and monitoring. The Interception and Monitoring Prohibition Act, 1992, was only made applicable to the whole territory of the Republic on 1 April 1997, when the Justice Laws Rationalization Act, 1996 (Act No. 18 of 1996), was put into operation. In drafting the Act, cognizance was taken of the legal position in Europe, Canada, the United States of America, Canada, standards of the European Court of Human Rights and specifically jurisprudence of the Court regarding interception and monitoring.

1.14 The fact remains, however, that in the meantime there was an interim Constitution, operative for a number of years and a final Constitution has been adopted. Furthermore, there have been considerable technological advances in respect of telecommunications - cellular communications, satellite communications, and computer communications through E-mail, and the electronic transfer of information and data.

1.15 There have also been considerable legal developments across the world regarding interception of communications - developments influenced by technology as well as financial considerations. The Irish Law Commission recently noted that the technological breakthroughs made in regard to surveillance have been spectacular:[6]

> "1.19 ... It is surprising if not shocking to learn of the ease with which this technology can pry open personal space which may previously have been considered safe. Specific examples of listening and optical surveillance devices which are generally available were listed by the Australian Law Commission as long ago as 1983. The gravity of surveillance as a threat to personal privacy in today's world can be understood from considering the following list:
>
> - parabolic microphones with ranges extending to more than 250 metres,
> - miniature tape-recorders which can be concealed inside, for example, cigarette packets,
> - binoculars having built-in cartridges,
> - listening devices laminated onto business cards,
> - brief-case cameras, activated by pressing a button on the briefcase,
> - residual light image intensifiers with ranges of up to 10 kilometres for long range observation at night,
> - day-and-night cameras connected to monitors and operated by remote control,
> - long-range photographic flash devices enabling photographs to be taken at night without detection and from a range of 100 metres or more,
> - microphones concealed in watches, buttonholes, pens and ties,
> - sub-miniature transmitters, smaller than sugar cubes, which can record conversations from a distance of 10 metres and transmit them at high quality up to 150 metres,
> - listening devices which through the use of laser beams can monitor and record conversations from positions outside the room in which they are occurring,
> - electronic stethoscopes which, by picking up mechanical vibrations and amplifying them up to 10,000-fold, enable conversations to be monitored through windows, doors and walls,
> - optical devices which permit continuous monitoring in complete darkness, and
> - listening devices placed in telephones, which enable surveillance of conversations within a room even when the telephone is not in use.
>
> 1.20 Indeed, the range and sophistication of technological devices which can be used

---

6 The Law Reform Commission *Report on Privacy: Surveillance and the Interception of Communications* June 1998 at 5 - 7.

for surveillance purposes have increased substantially since the Australian Law Reform Commission studied the topic of privacy, and technological innovation continues at an amazing rate. We pointed this out in our Consultation Paper and gave the following examples of recently developed surveillance devices:

- small video cameras which can be held in the palm of one's hand, and
- an artificial "eye" which, by a combination of optical computing and neutral networking, can "learn" to recognise objects in a way which mimics human sight.

1.21 More recently, surveillance technology is reportedly being developed using systems that can operate outside the visible light spectrum, such as:

- Forward-Looking Infra-Red systems which are able to detect human activity behind walls and
- Computerised Face Recognition technology which will enable the matching of an image on the street and a file on a database.

1.22 The next development in the technology will reportedly involve the development of an interactive link between surveillance technology and computerised data banks (CCTV surveillance networks). This will potentially allow for automatic tracking of the movements of individuals. Technology is already available to broadcast the footage generated by CCTV systems over the internet.

1.23 An enormous range of devices with extraordinary potential for intrusiveness (including for example a video camera in the form of a shower head) is now available cheaply by mail order over the internet, and there is a corresponding market in anti-surveillance devices similarly available. We allude in this report to copious accounts in the newspapers that sophisticated surveillance technology is being used in Ireland."

1.16 The Hong Kong Law Reform Commission recently considered the regulation of surveillance and interception of communications and examined, *inter alia*, the impact of new technologies on the ability to tap into telecommunications systems, and the competing ability to encrypt messages.[7] The Commission noted in regard to tappability that some new technologies such as optical fibres are making it harder to tap into telecommunications systems. They further stated that even where the communication is intercepted, modern technical developments in cryptography may preclude it from being deciphered. The Hong Kong Commission pointed out that the purpose of cryptography is the encrypting of information and that there is now easy availability of encryption sufficiently strong that an encrypted message would take the world's most powerful supercomputer years to crack. The Commission explained encryption as an accessible tool as follows:

9.32 Encryption software can be generated in less than 5 minutes with such simple equipment

---

7 Law Reform Commission of Hong Kong *Privacy: Regulating Surveillance and the Interception of Communications* Consultation Paper 1996 at http://www.info.gov.hk/info/pricon.htm accessed on 5/11/1998.

as PGP ("Pretty Good Privacy") software for e-mail and PGP Fone software for speech over a network using 2 Power Macintosh computers. PGP is the most popular system, being freely available to United States citizens in the United States and freely outside the United States, where it is not subject to patents. It is believed that the system is strong enough to resist challenge from most quarters, although it is impossible to prove how strong the system is, only how weak.

9.33 A vital feature of modern cryptography is that of the public keys. A lock-and-key approach is adopted to telecommunications security. The lock is a "public key", which a user can transmit to recipients. To unlock the message, the recipient uses a personal encryption code or "private key". The development of public key cryptography in the mid-1970s eliminated the need for network subscribers to provide trusted elements with the capability of decrypting any message. Public key encryption dramatically increases the availability of encryption/identification as the dual key system allows the encryption key to be made available to potential communicants while keeping the decryption key secret. This would allow, for example, a bank to make its public key available to many people, without those people being able to read each others' encrypted messages. Two relevant limitations, however, are:

(i) keys infrequently changed have an increased risk of being broken as, in principle, any public key system can be broken given sufficient computer power and time.

(ii) it is critical to ensure that the user has the correct public key. If provided by an intermediary, he could interpose a key of his own. Hence trust is a critical issue.

9.34 Another important feature of encryption is key signatures. These verify the identity of the person sending the message. They can be wiped after sending the message, so rendering it anonymous.

9.35 A system popular in the Hong Kong telephone market is that of Global System for Mobile communications (GSM) phones. The digital GSM technology employs a 54 bit encryption code: a single call would take a Cray supercomputer two hours to decipher.

1.17 Dr Duncan Chappell recently pointed out the effect of new technologies such as the launch of a new satellite telephone company Iridium would pose in regard to surveillance and interception.[8] He explained that the Iridium system is based on a constellation of 66 low earth orbit satellites which operate like a global cellular system, passing signals between them in a cell like formation so that a user can be reached anywhere in the world. Dr Chappell noted that this new development poses formidable challenges to those concerned in the investigation of crime, especially crime which transcends national boundaries:

> It must be presumed that not all of the targeted international business customers for these new satellite based personal communication systems will be law abiding citizens. These systems have obvious benefits for the conduct of both legitimate business enterprises, and a wealth of contemporary data and experience shows that criminals are enthusiastic consumers of new technologies like this which provide their nefarious activities with a fresh competitive edge. One competitive edge that a system like Iridium promises to give criminals is an ability to conduct

---

8 Deputy President: Administrative Appeals Tribunal of Sydney Australia in a paper presented at the Oxford Conference on International Co-operation in Criminal Matters: Balancing the protection of human rights with the needs of law enforcement (held from 24 - 28 August 1998) at 1 *et seq.*

their communications in an interception free environment. ... It is sufficient to highlight just one of the significant barriers which will confront the law enforcement community in gaining legal authority to intercept communications by persons subscribing to Iridium's services. Take, for example, an Australian subscriber who is believed, on reasonable grounds, to be involved in the importation from south East Asia of significant quantities of heroin. If an interception warrant were to be sought by an authorised law enforcement agency in Australia in regard to that subscriber, any execution of that warrant would have to involve the consent and agreement of a foreign government since the Iridium earth station gateway for Australia is located in India. Current mutual assistance arrangements between Australia and India do not extend to the interception of communications. While this situation is believed to be the subject of ongoing dialogue between governmental officials from the two countries it will almost certainly take some time to resolve the delicate legal and political issues involved.

Quite apart from this not insignificant barrier in Australia to the lawful interception of Iridium linked communications, and it must be presumed in many other countries which similarly lack an Iridium gateway on their own soil, there are also unresolved technological barriers to such interception ... remedies are being sought for these technological problems but in combination they provide a graphic illustration of the way in which the general revolution in communications is proceeding at such a pace that law enforcement interests and concerns are at best scrambling to remain in contention. As the authors of a recent study of "crime in the digital age" have remarked:

> ... [T]he advent of digital communications, combined with global trends towards privatisation and deregulation of the telecommunications industry, have posed new challenges for law enforcement. A proliferation of carriers and service providers may make it difficult to discern which one to approach for assistance in undertaking surveillance of a particular target. Moreover, telecommunication systems can be designed to be more or less accessible to interception. ...
> As if the above challenges were not formidable enough, they in turn are compounded by the increasing accessibility of encryption technology. ...
> In addition to encryption, law enforcement agencies are concerned about the development and convergence of other technologies such as digital compression, highspeed data links, multiplex cables, and asynchronistic transfer mode technology. These all contribute to reducing law enforcement access to voice and data transmissions. The democratisation of telecommunications technology, that is, its widespread accessibility to ordinary citizens, has begun to make many traditional law enforcement techniques obsolete.

1.18 Although, in democratic countries, the right to privacy of communications is generally accepted, it is also generally accepted that there are certain factors which demand a limitation of this right. Article 8 of the European Convention on Human Rights illustrates this point:

> "I. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> II. There shall be no interference by a public authority with the exercise of his right except such as is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

1.19 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data and the limitations to such protection is particularly noteworthy in this context:

Article 1 Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1. ...

Article 8 The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:
(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation ot professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.
Member States may provide that data relating to administrative sanctions or judgements in civil

cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed. ...

Article 13 Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:
(a) national security;
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

1.20 The protection of telecommunication data is particularly regulated in the European Community by Directive 97/66/EC of the European Council of 15 December 1997 concerning the Processing of Personal Data and Protection of Privacy in the Telecommunications Sector. The motivation for the Directive is set out, inter alia, as follows in the preamble to the Directive:

(2) Whereas confidentiality of communications is guaranteed in accordance with the international instruments relating to human rights (in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms) and the constitutions of the Member States;

(3) Whereas currently in the Community new advanced digital technologies are introduced in public telecommunications networks, which give rise to specific requirements concerning the protection of personal data and privacy of the user; whereas the development of the information society is characterized by the introduction of new telecommunications services; whereas the successful cross-border development of these services, such as video-on-demand, interactive television, is partly dependent on the confidence of the users that their privacy will not be at risk;

(4) Whereas this is the case, in particular, with the introduction of the Integrated Services Digital Network (ISDN) and digital mobile networks;

(5) Whereas the Council, in its Resolution of 30 June 1988 on the development of the common market for telecommunications services and equipment up to 1992, called for steps to be taken

to protect personal data, in order to create an appropriate environment for the future development of telecommunications in the Community; whereas the Council re-emphasized the importance of the protection of personal data and privacy in its Resolution of 18 July 1989 on the strengthening of the coordination for the introduction of the Integrated Services Digital Network (ISDN) in the European Community up to 1992;

(6) Whereas the European Parliament has underlined the importance of the protection of personal data and privacy in the telecommunications networks, in particular with regard to the introduction of the Integrated Services Digital Network (ISDN);

(7) Whereas, in the case of public telecommunications networks, specific legal, regulatory, and technical provisions must be made in order to protect fundamental rights and freedoms of natural persons and legitimate interests of legal persons, in particular with regard to the increasing risk connected with automated storage and processing of data relating to subscribers and users;

(8) Whereas legal, regulatory, and technical provisions adopted by the Member States concerning the protection of personal data, privacy and the legitimate interests of legal persons, in the telecommunications sector, must be harmonized in order to avoid obstacles to the internal market for telecommunications in conformity with the objective set out in Article 8a of the Treaty; whereas the harmonization pursuant to the principle of subsidiarity is limited to requirements that are strictly necessary to guarantee that the promotion and development of new telecommunications services and networks between Member States will not be hindered;

(9) Whereas the Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by the provisions of this Directive;

(10) Whereas these new services include interactive television and video on demand;

(11) Whereas, in the telecommunications sector, in particular for all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals, Directive 95/46/EC applies; whereas Directive 95/46/EC applies to non-publicly available telecommunication services;

(12) Whereas this Directive, similarly to what is provided for by Article 3 of Directive 95/46/EC, does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law; whereas it is for Member States to take such measures as they consider necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law; whereas this Directive shall not affect the ability of Member States to carry out lawful interception of telecommunications, for any of these purposes;

(13) Whereas subscribers of a publicly available telecommunications service may be natural or legal persons: whereas the provisions of this Directive are aimed to protect, by supplementing Directive 95/46/EC, the fundamental rights of natural persons and particularly their right to privacy, as well as the legitimate interests of legal persons; whereas these provisions may in no case entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the legitimate interests of legal persons; whereas this protection is ensured within the framework of the applicable Community and national legislation; ...

1.21 Directive 97/66/EC provides in article 5(1) that Member States shall ensure via national regulations the confidentiality of communications by means of public telecommunications

network and publicly available telecommunications services, and in particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications, by others than users, without the consent of the users concerned, except when legally authorized. It also makes provision in article 5(2) that paragraph (1) shall not affect any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication. It further provides in article 14(1) that Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 5, 6[9] and Article 8(1),[10] (2),[11] (3)[12] and (4),[13] when such restriction constitutes a necessary measure to safeguard national security,

---

9 6(1) Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.
(2) For the purpose of subscriber billing and interconnection payments, data indicated in the Annex may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued. [The list of data set out in the Annex is - data containing the number or identification of the subscriber station; address of the subscriber an the type of station; total number of units to be charged for the accounting period; called subscriber number; type, starting time and duration of the calls made and/or the data volume transmitted; date of the call/service; other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.]
(3) For the purpose of marketing its own telecommunications services, the provider of a publicly available telecommunications service may process the data referred to in paragraph 2, if the subscriber has given his consent.
(4) Processing of traffic and billing data must be restricted to persons acting under the authority of providers of the public telecommunications networks and/or publicly available telecommunications services handling billing or traffic management, customer enquiries, fraud detection and marketing the provider's own telecommunications services and it must be restricted to what is necessary for the purposes of such activities.
(5) Paragraphs 1, 2, 3 and 4 shall apply without prejudice to the possibility for competent authorities to be informed of billing or traffic data in conformity with applicable legislation in view of settling disputes, in particular interconnection or billing disputes.

10 Where presentation of calling-line identification is offered, the calling user must have the possibility via a simple means, free of charge, to eliminate the presentation of the calling-line identification on a per-line basis, and that the calling subscriber must have the possibility on a per-line basis.

11 Where presentation of calling-line identification is offered, the called subscriber must have the possibility via a simple means, free of charge for reasonable use of this function, to prevent the presentation of the calling line identification of incoming calls.

12 Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the called subscriber must have the possibility via a simple means to reject incoming calls where the presentation of the calling line identification has been eliminated by the calling user or subscriber.

13 Where presentation of connected identification is offered, the called subscriber must have the possibility via simple means, free of charge, to eliminate the presentation of the connected line

defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the telecommunications system, as referred to in Article 13(1) of Directive 95/46/EC.

1.22 The following recommendation[14] made on 3 May 1999 by the Working Party on the protection of individuals with regard to the processing of personal data, instituted by Directive 95/46/EC of the European Council, of 24 October 1995, highlights problematic issues in regard to interception of telecommunications and the right to privacy:

> The purpose of this recommendation is to indicate how the principles on the protection of the fundamental rights and freedoms of natural persons, and in particular of their privacy and the secrecy of their correspondence, is to be applied to the measures concerning the interception of telecommunications adopted at European level.
>
> This recommendation covers interception understood in a broad sense, i.e. not only of the contents of telecommunications, but also of any related data, particularly any preparatory measures (such as monitoring and determining traffic data) which may be envisaged in order to determine whether intercepting the contents of a telecommunication is advisable .
>
> A. Scope of the provisions on the interception of telecommunications adopted at European level
>
> 1. The Council Resolution of 17 January 1995 on the lawful interception of telecommunications lists the technical conditions required for the interception of telecommunications, without going into the conditions under which such interception may be permitted. The Resolution requires network operators or service providers to pass the intercepted data on to the "authorised services" in plain text.
> The data concern telephone calls, whether from mobiles or conventional units, e-mail, faxes and telex messages, and Internet data traffic, with regard to both content and any data related to telecommunications (this refers particularly to traffic data, but also to any signal transmitted by the person under surveillance - point 1.4.4. of the Resolution).
> Data are to be collected both on the target persons and on any persons with whom they enter into communication.
> The Resolution also provides for law enforcement agencies to have access to data on the geographical location of a mobile subscriber .
> The Resolution of 18 January 1995 is currently being revised, with one of the main goals being to adapt it to new communication technologies. In particular, the draft text addresses how to apply interception measures to satellite telecommunications.
>
> 2. The Working Party is concerned about the scope of the measures envisaged by the Council Resolution of 17 January 1995. An unpublished, more recent version of the document referred to above ("declaration of intent" dated 25 October 1995), provides for the signatories to the text to contact the director of the United States Federal Bureau of Investigation about the requirements for the interception of telecommunications. The text also provides, subject to the approval of the "participants", for other States to take part in the exchange of information and in the revision and updating of the requirements.
> The Working Party points out that the legal status of this text is unclear - particularly as regards the actual signing by the countries concerned - and that it does not constitute a measure

---

identification to the calling user.

14 Recommendation on the Respect of Privacy in the context of Interception of Telecommunications.

accessible to the citizen according to the case law of the European Court of Human Rights quoted below, insofar as it has not been published. Secondly, the text notes a desire to develop technical measures for intercepting telecommunications jointly with States which are not subject to the requirements of the European Convention on Human Rights and of Directives 95/46/EC and 97/66/EC.

3. The Working Party notes that the Council Resolution aims to settle technical questions on the means of intercepting communications, without affecting the national provisions which regulate phone tapping in legal terms. Nonetheless, certain measures the resolution provides for, which increase the scope for intercepting telecommunications, conflict with the more restrictive national regulations of certain countries in the European Union (particularly point 1.4, access to data concerning calls, including calls from mobile phones, without considering the anonymous prepaid services now available; point 1.5, geographical location of mobile subscribers, and point 5.1, forbidding operators from disclosing interceptions after the fact.)

4. Although the Council Resolution is in line with an aim of 'the protection of national interests, national security and the investigation of serious crimes', the Working Party wishes to draw attention to the risks of abuses with regard to the objectives of tapping, risks which would be increased by an extension to a growing number of countries - some of which are outside the European Union - of the techniques for intercepting and deciphering telecommunications.
A European Parliament resolution of 16 September 1998 relating to transatlantic communications 'considers that the increasing importance of the Internet network, and more generally of telecommunications on a world-wide scale and in particular the Echelon system, as well as the risks of their abuse, call for the adoption of measures to protect economic information and effective encoding'.
These considerations highlight the risks associated with telecommunication interceptions which go beyond the strict framework of questions of national security - and thus fall outside the European Union's 'third pillar'. They raise the question of their legitimacy, in particular in the light of the obligations arising from Community legislation on the protection of the fundamental rights and freedoms of natural persons, particularly their privacy.

5. The Working Party emphasises, finally, that as a result of the Treaty of Amsterdam coming into force, the legal basis of provisions for the interception of telecommunications will change at European level. The basis for the Council to draw up the resolution (currently articles K.1 (9) and K.3 (2) of the Treaty on police and judicial co-operation), will include powers of initiative of the European Commission under the new article K.6 (2).

B. General Legal Framework

6. The Working Party points out that each telecommunication interception, defined as a third party acquiring knowledge of the content and/or data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunication services, constitutes a violation of individuals' right to privacy and of the confidentiality of correspondence. It follows that interceptions are unacceptable unless they fulfil three fundamental criteria, in accordance with Article 8 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, and the European Court of Human Rights' interpretation of this provision: a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention. The legal basis must precisely define the limits and the means of applying the measure through clear and detailed rules which are particularly necessary owing to the continuous improvement of the technical means available . The text of the law must be accessible to the public so that citizens may be informed of the consequences of their behaviour.

In this legal context, exploratory or general surveillance on a large scale must be proscribed.

7. Within the European Union, Directive 95/46/EC establishes the principle of the protection of the right to privacy enshrined in the legal systems of the Member States. This Directive specifies the

principles contained in the European Convention for the Protection of Human Rights of 4 November 1950 and in Council of Europe Convention No. 108 of 28 January 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Directive 97/66/EC gives concrete expression to the provisions of this Directive by specifying the Member States' obligation to ensure through national regulations the confidentiality of communications carried out by means of a public telecommunications network or by means of publicly available telecommunication services.
According to Article 13 (1) of Directive 95/46/EC, Member States may adopt legislative measures to restrict the scope of certain obligations (for example, concerning the collection of data) and certain rights (for example, the right to be informed of data collection) provided for in the Directive. These exceptions are strictly enumerated: the restriction must constitute a measure needed to safeguard the public interests exhaustively listed in paragraphs a) to g) of this article, which include national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.
Article 14 (1) of Directive 97/66/EC similarly states that Member States may only restrict the obligation of the confidentiality of communications on public networks when such a measure is required to safeguard national security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences.

C. Obligations of Telecommunications Operators and Service Providers

8. It must be stressed that the obligations of the security and confidentiality of data to which telecommunication operators, service providers and Member States are subject on the basis of Articles 17 (1) and (2) of Directive 95/46 and Articles 4, 5 and 6 of Directive 97/66/EC respectively are the rule and not the exception.
The Working Party points out that these obligations also apply to operators in general under Article 7 of Council of Europe Convention No. 108 of 28 January 1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data, and Article 4 of the Council of Europe Recommendation No. 4 of 7 February 1995 on the Protection of Personal Data in the Field of Telecommunication Services, with particular regard to telephone services.

9. These obligations imply that telecommunications operators and telecommunications service providers may not process data on telecommunications traffic and billing except under certain conditions: given that traffic data on subscribers and users must be erased or made anonymous as soon as the communication ends, it follows that the purposes for which the data may be processed, the length of time they may be kept (if at all) and access to them must be strictly limited .

10. Telecommunications operators and telecommunications service providers must take the measures needed to make the interception of telecommunications by unauthorised parties impossible, or as technically difficult as the current state of the technology allows.
The Working Party stresses in this respect that the implementation of effective means of intercepting communications, using precisely the most advanced techniques, must not result in a lowering of the level of confidentiality of communication and protection of the privacy of individuals.
These obligations take on a special meaning when telecommunications between individuals located on the territory of the Member States pass or may pass outside European territory, in particular when satellites or the Internet are used.

11. Where Directive 95/46 applies, making such telecommunications accessible outside the European Union could moreover constitute a violation of Article 25 of the Directive, insofar as foreign authorities intercepting them may not be able to ensure an adequate level of data protection.

D. Respect of Fundamental Freedoms by the Authorities with regard to Interceptions

12. Taking into account the above-mentioned provisions, it is important for national law to strictly specify:

- the authorities responsible for permitting the legal interception of telecommunications, those authorised to carry them out and the legal basis for their action,
- the purposes for which such interception may be carried out, which allow an assessment of whether it is proportionate to the national interests at stake,
- the prohibition of all large-scale exploratory or general surveillance of telecommunications,
- the exact circumstances and conditions (for example, facts justifying the measure, duration of the measure) governing the interceptions, without violating the principle of specificity which any interference in the privacy of individuals must respect ,
- compliance with the principle of specificity, which is a corollary of forbidding all exploratory or general surveillance. Specifically, as far as traffic data are concerned, it implies that the public authorities may only have access to these data on a case-by-case basis, and never proactively and as a general rule.
- the security measures for the processing and storage of the data, and the length of time data may be kept,
- the guarantees concerning the processing of data concerning individuals affected indirectly or by chance by interceptions, in particular the criteria used to justify the conservation of data, and under what conditions these data may be passed on to third parties,
- that a person under surveillance be informed of this as soon as possible,
- the recourse available to a person under surveillance ,
- the arrangements for the monitoring of these services by an independent supervisory authority.
- publication of the policies on the interception of telecommunications as they are actually practiced, for example, in the form of regular statistical reports,
- the specific conditions under which the data may be transmitted to third parties under bilateral or multilateral agreements.

1.23 The provisions of the European Conventions on Human Rights and Data Protection, the Directive and the Recommendation issued in regard to the last mentioned Convention are of particular importance for the South African situation for the following reasons:

(a) Section 14 of the Constitution of the Republic of South Africa, 1996 (Act No. 108 of 1996) guarantees as a fundamental right, the right to privacy, which includes the right not to have "the privacy of their communications infringed."

(b) The limitations clause in the Constitution provides that the rights in the Bill of Rights (in which section 14 is included), "may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors ...."

1.24 The following observation was made in the *Naidoo* case regarding the constitutionality of the Interception and Monitoring Act, 1992:[15]

> "What is clear is that, probably after the experience of police methods during the apartheid era, ... the Legislature saw fit to repeal the old provisions relating to interception of personal articles, telephone communications, etc. in terms of which various Ministers could authorize such actions and to replace those provisions with the obviously extremely stringent and limited provisions of the Monitoring Act. Such provisions are, as I have already indicated, in line with similar provisions in other countries...."

1.25 The court also remarked that a concession by the counsel for the defence that the Monitoring Act was a law of general application, the provisions of which complied with the requirements of section 33 of the interim Constitution, was in his view "properly made".

1.26 It would seem as if the right to the privacy of telecommunications in some respects finds more favourable recognition in the ECHR and for example the German Basic Law, than in the United States of America.[16] The Data Protection Working Party[17] recently remarked as follows[18]:

> Data protection rules are not only intended to protect users of new technologies (in particular informatics and Internet) with a view to guaranteeing trust and confidence and thus to provide for the development of these technologies and the exchange of data at international level. These rules express also the adherence to a certain number of fundamental principles and rights based on a common culture of respect for privacy and other values that are inherent in the human being and which is shared equally by the Member States of the European Union and the United States.
>
> 1. Privacy and data protection in the United States is found in a complex fabric of sectoral regulation, at both federal and state level, combined with industry self-regulation. Considerable efforts have been made during recent months to improve the credibility and enforceability of industry self-regulation, particularly in the context of the Internet and electronic commerce. Nevertheless, the Working Party takes the view that the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate

---

15 S v *Naidoo and Another* [1998] 1 All SA 189 on 213.

16 Blanca R Ruiz "Privacy in Telecommunications. An European and an American approach." Kluwer Law International. The Hague 1997, p.175, 176: "Finally in one important respect the recognition of the right to secrecy of telecommunications in the ECHR and Germany is more favourable to the right than its recognition in the United States. This concerns the relation existing between the secrecy of telecommunications as a fundamental right and privacy as the interest lying behind it."

17 Instituted by Directive 95/46/EC of the European Council of 24 October 1995.

18 Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government adopted by the Working Party on 26 January 1999.

protection in all cases for personal data transferred from the European Union.

2. Given the complexity of the US system of privacy and data protection, the establishment in the US of an agreed "benchmark" standard of protection in the form of a set of "safe harbor" principles offered to all economic actors and US operators is a useful approach which might need to be complemented by contractual solutions in certain specific cases. However, further improvements are needed if free movement of data to the United States is to be ensured on the basis of these privacy principles. In addition, it might be necessary to provide for a methodology which makes clear which companies are covered by the "safe harbor" principles.

3. It has to be noted that the decision to adhere to the set of principles belongs solely to the individual company, and so the problem of those companies which do not wish to apply the principles remains whilst no overall legislation exists.

4. Generally, the status of these principles needs to be clarified. Whilst adherence to the principles in the first instance can be voluntary, once a company does decide to adhere and thereby to claim the benefit of "safe harbor", compliance must be compulsory.

5. The credibility of the system is seriously weakened by the lack of a requirement for independent compliance monitoring and by relying solely on company self-certification. Independent verification would need to be serious but could at the same time be practicable, even for small companies. Models currently being developed in the US by the Better Business Bureau OnLine and Trust-E are going in the right direction.

6. It must be possible for complaints from individuals whose data have been transferred from the EU to be dealt with in a practical and effective manner, and adjudicated upon, in the final instance, by an independent body. A key issue in this regard is the identification of one or more independent public bodies or third party organisations in the US that are willing and able to act as contact points for EU data protection authorities and to co-operate in the investigation of complaints. Care must be taken to ensure that practical arrangements are in place for all relevant US sectors. Existing regulatory agencies, such as the Federal Trade Commission and the Office of the Comptroller of the Currency can perform such a role in the areas for which they have competence.

7. In terms of its substantive content, any acceptable set of "safe harbor" principles must, as a minimum requirement, include all the principles set out in the OECD Privacy Guidelines of 1980, adopted amongst others by the United States and recently re-endorsed at the OECD's Ottawa Conference on Electronic Commerce. These principles are also applied by Directive 95/46/EC as well as by national legislation of the Member States of the European Union. In this regard, the above mentioned consultative text of principles published by the US Department of Commerce on 4 November 1998 raises some concerns, in particular:

a) The individual's right of access is limited to that which is "reasonable". The OECD Privacy Guidelines do not limit the right itself, simply asserting that it must be exercised "in a reasonable manner".

b) The purpose specification principle of the OECD Privacy Guidelines is absent, and is only partly replaced by a "choice" principle which in effect allows data collected for one purpose to be used for another, provided individuals have the possibility of opting out.

c) Proprietary data and any manually processed data are entirely outside of the scope of the US principles, while the "choice" principle provides no protection to data collected from third parties and the "access" principle excludes public record-derived information.

d) According to the third paragraph of the introduction, "adherence to the principles is subject to" a number of exceptions and limitations such as "risk management" and "information security". The

Working Party takes the view that these notions are too vague and open-ended, and recommends that they be clarified or deleted.

1.27 There is, in view of the factors set out above, a more compelling reason to review the Interception and Monitoring Prohibition Act, 1992, from a legal point of view. Telecommunications are being used more and more in the organizing and commissioning of crime, especially organized crime, heists and other serious violent crimes. Legal provision should be made to give law enforcement agencies the necessary tools to investigate such crimes as well as other concomitant crimes such as money-laundering. A review of the Act should ensure that the emphasis in the Act should be on crime.

CHAPTER 2

THE LEGAL POSITION IN SOUTH AFRICA

2.1 It has already been pointed out that the right to privacy of communications is a fundamental right, protected in the Bill of Rights (section 14 of the Constitution).

2.2 The Interception and Monitoring Prohibition Act, 1992, is an Act of general application, which provides for the limitation of the above right.

2.3 The Interception and Monitoring Prohibition Act provides for the designation, by the Minister of Justice of a judge in a local or provincial division of the High Court to consider applications for interception and monitoring. In practice, however, only one judge has been appointed for all the Divisions and all applications for interception and monitoring are being considered by that judge. This has been the position since the putting into operation of the Act. It may be argued that, in terms of section 6(b) of the Interpretation Act, 1957 (Act No. 33 of 1957), the reference to the singular in any Act, also includes the plural, unless the contrary is evident from the wording of the Act. Further that there is no reason evident from the Act why a separate judge has to be appointed for each division. In view of these arguments a single judge may be designated for two or more, or all the divisions of the High Court, so long as the designation is linked to divisions.

2.4 There is no differentiation in South Africa regarding the consideration of national security and applications relating to crime investigations for interception and monitoring, respectively: the same judge considers all applications.

2.5 The Interception and Monitoring Prohibition Act, 1992, prohibits -

(a) the interception of a communication which has been or is intended to be transmitted by telephone or in any other manner over a telecommunications line, intentionally and without the knowledge or permission of the dispatcher;

(b) the intentional monitoring of a conversation or communication[19] by means of a

---

19 See the amendments in the Judicial Matters Amendment Act, 1998 (Act No. 34 of 1998).

monitoring device so as to gather confidential[20] information concerning any person, body of organization.

2.6 The Act further provides for a mechanism to obtain a direction to intercept/monitor communications. A designated judge may direct that -

(a) a particular postal article or a particular communication which has been or is being or is intended to be transmitted by telephone, or in any other manner over a telecommunication line be intercepted;

(b) all postal articles to or from a person, body or organization or all communications which have been or are being or are intended to be transmitted by a telephone or in any other manner over a telecommunication line, to or from a person, body or organization be intercepted;

(c) conversations or communications by or with a person, body or organization, whether a telecommunications line is being used in conducting those conversations or communications or not, be monitored in any manner by means of a monitoring device.

2.7 A direction to intercept/monitor a conversation/communication may be issued by a designated judge if the judge is convinced -

- that a serious offence has been committed or is being or will probably be committed, which cannot be investigated in any other manner and of which the investigation in terms of the Act is necessary; or
- that the security of the Republic is threatened or that the gathering of information concerning a threat to the security of the Republic is necessary.

2.8 A **"serious offence"** is defined in the Act as -

---

20 The Act does not define "confidential" information, but in the case of *Protea Technology Limited and Another v Wainer and Others* [1997] 3 A11 SA 594 on 603, the court remarked as follows:

"That expression must surely mean such information as the communicator does not intend to disclose to any person other than the person to whom he is speaking and any other person to whom the disclosure of such information is necessary or impliedly to be restricted. I think that there is a distinction between 'confidential' information and 'private' information."

"(a) any offence mentioned in Schedule 1 of the Criminal Procedure Act, 1977 (Act No. 51 of 1977), including any conspiracy, incitement or attempt to commit any offence referred to in that Schedule, provided that -

(i) that offence is allegedly being or has allegedly been committed over a lengthy period of time;

(ii) that offence is allegedly being or has allegedly been committed on an organized basis, by the person or persons involved therein;

(iii) that offence is allegedly being or has been committed on a regular basis by the person or persons involved therein; or

(iv) that offence may allegedly harm the economy of the Republic; or

(b) any offence referred to in sections 13(f) and 14(b) of the Drugs and Drug Trafficking Act, 1992."

2.9 The Act does not provide for once-off murder, rape, robbery, etc unless committed in an organized fashion - which may be a serious defect in terms of the high incidence of serious violent crime in South Africa. The court found in the *Naidoo* case,[21] that it would be absurd to suggest that an offence provided for in Schedule 1 would only be regarded as a serious offence if it complied with all the requirements of subparagraphs (i), (ii) and (iii): "Those three paragraphs seem to me to contemplate three different ways of committing a serious crime such as referred to in Schedule 1 to the Criminal Procedure Act". The three paragraphs should, in the court's view, be read in the disjunctive. The court remarked as follows:[22]

> "As it is, it seems to me that the requirements of the proviso to paragraph (a) of the definition of "serious crime" are unduly restrictive and likely to impede the proper investigation of some crimes in South Africa. If paragraph (a) of the definition is to be interpreted so as to require compliance with (i) and (ii) and (ii) or (iv) there would not be many offences mentioned in Schedule 1 to the Criminal Procedure Act, 1977, which could be the subject of a direction by a judge as contemplated in sections 2 and 3."

2.10 An internal, departmental approval to apply to the designated judge is prescribed by the Act. A member of the institution concerned applying for a direction from the designated judge, has to obtain the permission of, in the case of the South African Police Service, an assistant

---

21 Supra at p 214.

22 At p 214.

commissioner or a member on the same rank, in the case of the South African National Defence Force of an officer with the rank of major-general, and in respect of the National Intelligence Agency or the South African Secret Service, a member holding a post of at least chief director. In the cases of the South African Police Service and the South African National Defence Force, the officials authorizing the application to the judge, have to be specifically designated by the National Commissioner of the South African Police Service and the Chief of the South African Defence Force, respectively.

2.11 A direction for interception and monitoring may be approved by the Judge for a maximum period of three months and thereafter for a further period not exceeding three months at a time, if the judge is convinced that the extension is necessary for a reason mentioned in section 3(1)(b)(i) or (ii) (serious crime or national security).

2.12 A direction may be executed by a member of the institution concerned, authorized by the officer or member who made the application for the direction. A member who executes a direction or assists with the execution of a direction may at any time enter upon any premises in order to install, maintain or remove a monitoring device, or to intercept or take into possession a postal article, or to intercept any communication, or to install, maintain or remove a device by means of which any communication can be intercepted, for the purposes of the Act.

2.13 In terms of section 5 of the Act any person rendering a postal or telecommunications service is obliged to intercept any telegram or postal article to which the direction applies and hand it over to the member who is authorized to execute the direction. The necessary facilities and devices to enable the member who is authorized to execute a direction must be made available to effect the necessary connections in order to monitor conversations to which the direction applies.

2.14 If a person, body or organization has made a facility, device or telecommunications line available, for the purposes of the Act, the remuneration agreed upon by the person or organisation and the Commissioner of the South African Police Services, the Chief of the South African Defence Force or the Director -general of the Agency or Service, as the case may be, shall be paid to that person, body or organisation for assisting to execute a direction. If no agreement can be reached, a reasonable remuneration must be determined by the Minister for Posts, Telecommunications and Broadcasting with the concurrence of the Minister for State

Expenditure in order to compensate the person, body or organisation at least for any costs incurred as a result of any action taken in terms of the Act.

2.15 The Judges-President of the High Court may jointly issue and have jointly issued directives in which the manner and procedure of applications in terms of the Act are uniformly regulated.

2.16 There is a prohibition on the disclosure of any information regarding or gained from interception and monitoring, save for disclosing -

(a) it to any person who of necessity requires it for the performance of his or her functions in terms of this Act;
(b) it if he or she is a person who of necessity supplies it in the performance of his or her functions in terms of the Act;
(c) such information which is required in terms of any law or as evidence in any court of law;
(d) it to any competent authority which requires it for the institution, or an investigation with a view to the institution, of any criminal procedure.

2.17 Penalties are provided for unlawful interception or monitoring (a fine or imprisonment for a period not exceeding two years) and for unauthorized disclosure of information regarding or obtained from interception or monitoring to a fine or imprisonment for a period not exceeding five years. The communications/conversations between an attorney and his client are privileged, and may not be intercepted/monitored.[23]

2.18 There have been requests especially from anti-corruption units to authorize the monitoring of telephone conversations in police institutions on the basis that personnel be informed that their conversations/communications may be monitored. The argument was that such personnel would not have a legitimate expectantion of privacy. (The basis for these arguments could be found in the *Protea* case.) The following arguments can be raised against

---

23 *S v Nkabinde and Another*. Case no. CC 124/97 Pietermaritzburg High Court Judge Combrink "But, I can find no provision in that Act, which would entitle the police to intercept communications between an accused person and his legal representatives, and that cannot have been the Legislature's intention in enacting that measure."

such a practice:

* Section 2(1)(b) of the Act, only refers to the intent to "gather confidential information of a person, body or organization, unlike section 2(1)(a) which refers to "without the knowledge or permission of the dispatcher of a communication".
* In the Protea case[24] it is stated that "The language of subsection 1(a) points to the sending of telegrams, telefaxes and other similar means of transmission of messages (which seems inappropriate to a person speaking in a telephone), 'communication' (which, in the definition of "telecommunications line" in section 1 is distinguished from 'sound' and 'intercept' (which bears the meaning here to check, cut off (the passage from one place to another), and seems inappropriate to a spoken communication), as well as the fact that subsection (1)(b) is in specific terms directed to a spoken communication. The Shorter Oxford English Dictionary defines monitor as 'to listen to and report on (radio broadcasts, especially from a foreign country); also to eavesdrop on (a telephone conversation).' Dictionaries published in the United States furnished a meaning 'to keep track of by means of an electronic device' or 'to scrutinize or check systematically (with a view to collecting certain data).' These definitions accord with that in section 1 of the Act: **"Monitor"** includes the recording of conversations by means of a monitoring device."
* It seems, however, that if a party to a conversation gives his explicit permission for a conversation to be monitored, whether in a normal conversation or telephone conversation, that the prohibition in the Act would not be applicable. With reference to a call from a person demanding ransom, the judge mentioned that "it appears to me that they might escape the prohibition in section 2(1)(b) of the Act on the grounds of consent by one of the parties to the telephone call." (p. 213).

2.19 The last-mentioned ground does not seem to provide justification to monitor the telephones in a police office only on the basis of a notification to members, especially if that information is to be used in a criminal prosecution as evidence. It would seem as if monitoring in these circumstances should be clearly regulated by the Act.

---

24 Supra at p 603 (a-d).

2.20 This practice does exist in some countries, e.g. Britain. The British Interception of Communications Act, 1985, does not apply to "internal" communications, that is communications systems outside the public network such as a police station. In the case of *Halford v United Kingdom*[25] the court found as follows:

> "In particular, in the area of covert surveillance and interception of communications, where there was a lack of public scrutiny and the risk of abuse by public authorities, the domestic law had to afford citizens an adequate indication as to the circumstances and conditions under which the authorities were empowered to resort to such secret measures. It followed that the absence of regulation of the surveillance of internal communications systems under the domestic law, in the instant case, meant that the applicant was not adequately protected against interferences by the police with her right to respect for her private life and correspondence and that there had therefore been a violation of articles 8 and 13 of the Convention, in relation to the interception of the calls, made on her office telephones."

2.21 It seems that if the issue of monitoring communications on internal telephones were to be regulated properly by law, it might very well be permissible without contravening the European Convention on Human Rights. The question arises of whether this issue should be sanctioned, especially in view of the prevalence of corruption in government, secured environments such as intelligence and the military, and the need to monitor official telephones to ensure that employees do not act against the interests of their employers. It seems, in view of the *Protea* case that the principle has been accepted in the case of businesses.[26] This matter is probably an emotional policy issue which needs to be considered carefully. Flowing from the *Halford* case, it may be argued that a notification that the calls made from the facilities of a business or institution will be monitored, should be specific rather than general.

2.22 In the *Naidoo* case[27] the court was in favour of excluding evidence obtained in violation of any right in the Bill of Rights. The court was satisfied that the admission of the telephonic

---

25 (1997) 3 B HRC 3 (European Court of Human Rights).

26 Supra at p 608 - 609 (a-b). "The first respondent was employed by the applicants in a position of trust. The telephone conversations were conducted from the applicant's business premises within business hours. The applicants were entitled to require the first respondent to account for his activities during their time. (It will be recalled, in addition that the first respondent was contractually obliged to devote his full attention to the affairs of the group). It may be accepted that, even in this context, and within reason and at the direction of the employer, an employee's private life is not excluded. Thus he may receive and make calls which have nothing to do with his employers business. The employee making such calls has a legitimate expectation of privacy."

27 *Supra* at p 210, 211.

conversations in question would render the trial unfair. In this case the direction for monitoring was obtained by submitting false evidence to the judge.

2.23 A matter which is alarming in South Africa, is the large number of advertisements, sometimes even in law journals of private investigators, offering to deliver services which include "bugging". In view of the fact that only the South African Police Service, the South African Secret Service, the South African National Defence Force and the National Intelligence Agency may be authorized to do interception and monitoring, the legality of monitoring in certain circumstances by private investigators is questionable, especially in regard to instances of third party monitoring.

2.24 In the United States of America the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices are prohibited.[28] The devices in question are devices which "render it primarily useful for the purpose of the surreptitious interception of wire or oral communications". It is accepted that video and recording equipment may be misused for the purpose of illegal and " surreptitious" monitoring and that the policing of such a prohibition might be problematic. The Irish Law Reform Commission notes that the trade in surveillance devices is regulated in France by decree.[29] Provision was made for a list of devices intended to pick up conversations at a distance after consultation with the *Conseil d'Etat* subjecting the manufacture, importation, possession, display, offering, rental or sale of devices on the list to ministerial authorisation the granting of which was subject to conditions laid down by decree. The Irish Law Reform Commission however points out that no list of devices has been drawn up as of 1 January 1995.

2.25 It was therefore suggested in the discussion paper that the aspect of the manufacture, importation, possession, display, offering, rental or sale of surveillance devices should be carefully considered with a view to consider whether a regulatory provision such as that of the USA should not be included in South African law.

---

28 Section 2512 of the Omnibus Crime Control and Safe Streets Act.

29 *Report on Privacy: Surveillance and the Interception of Communications* at 95 - 96.

CHAPTER 3

THE LEGAL POSITION IN FRANCE

3.1 In April 1990, the European Court of Justice condemned France that there was no guarantee of human rights in France, regarding the interception of communications. On 10 July 1991, an Act was published in the Gazette, which provides the legal framework for security interceptions.[30]

3.2 There is a dual system of authorisation of interception of communications in France. It is accepted that in a democracy it is still necessary to have the power to intercept communications, with the necessary authority and for specified purposes such as law enforcement and the security of the public. Very strict rules have been created in order to control the use of interception in order to ensure its legality. Firstly there is the administratively authorised interception, which may only be used for a period of four months, for security reasons, namely to protect the democracy, to fight terrorism and organised crime and to protect important information relating to national security, the economy of France, counter-espionage and subversion. Political party activities may not be monitored. The Minister of the Interior must request authorisation for this type of interception from the Prime Minister, who is empowered by law to authorise such interception.

3.3 An annual report has to be submitted by the Prime Minister to a special committee, called the *Commission nationale de contrôle des interceptiones de securité*, to review whether sufficient grounds existed for the authorisation of the interception. The Committee is independent and is appointed for a period of six years at a time. The Commission has wide powers and may ask for further information on a specific case. It may instruct the Prime Minister at any time to terminate an interception. Although the Prime Minister is not bound to the recommendation of the Committee, it is difficult for the Prime Minister not to comply. The power of the Committee lies in its annual Report, which is published at the end of January. In the past the Prime Minister has always followed the recommendations of the Committee. The press also fulfils a watchdog function to ensure compliance to the recommendations of the

---

30 Loi no 91 - 646 du 10 Juillet 1991 relative an secret des correspondances émises par la voice des telecommunications.

Committee.

3.4 An administrative monitoring is admissible for a maximum period of four months. It is only as an exception renewed for another four months. A fresh application must be lodged for a renewal, setting out good reasons. The information obtained from administrative or security monitoring, may not be used as evidence in court. Hence, administratively authorised monitoring is used less often. The Judicial Police for example may use a quota of 300 per year, but never fully uses that quota, because it is frustrating not to be able to use the evidence in court. Authorisation for judicially obtained monitoring is easily obtained and implemented. In the case of the judicial police, security monitoring is only used for preliminary investigations. If after 4 months no evidence is found, the monitoring is terminated. If sufficient information results from the monitoring, the Judge is approached to obtain a warrant for a judicial monitoring. In the case of the judicial police, statistics have shown that more than 50% of administrative monitoring is eventually transformed to judicial monitoring.

3.5 Secondly, there is interception authorised by an investigation judge. The judge has to indicate in his authorisation who may be monitored, the grounds on which the person may be monitored, and the period of monitoring. This type of monitoring is only permissible in cases of crimes punishable with imprisonment for a period of 2 years. When the recordings of communications are to be used as evidence, every communication which has been monitored, has to be provided to the defence lawyer on request. No recordings may be destroyed before the finalisation of a criminal trial. If there is no criminal trial, the recordings may not be destroyed before 20 years have elapsed after the recording has been made.

3.6 An administrative monitoring may be transformed into a judicial monitoring by an application to the instructing judge, but a judicial monitoring may not be transformed to an administrative one. A judicially authorised monitoring may be executed for a maximum period of 12 months. During 1991 it was decided that there is no duty to inform any person that his or her communications have been administratively or judicially monitored. This is unlike the position in the Netherlands, Germany and Belgium where there is a duty of disclosure.

3.7 There is no distinction between the various forms of communications which may be monitored, therefore all forms of communications, namely satellite, fax, data, GSM mobile phones, fixed telephones, etc. may be monitored. Judicial authorisation for monitoring is not

subjected to scrutiny by the Commission which scrutinises the administrative authorisation for interceptions.

3.8 Entry for purposes of executing an authorisation for interception is not regulated in the law concerned. Service providers of communication networks are responsible to execute authorisations concerning telecommunication interceptions. Only the police service may make use of judicial authorisation for monitoring. Communications between a lawyer and his client are privileged, and may not be monitored. Where a lawyer is involved in crime, his communications may be monitored, but the chairman of the association of lawyers (the "batogne") for that area has to be notified that a lawyer is being monitored.

3.9 The distribution of quotas in regard to interceptions are as follows:

*	National Police	:	1200;
*	Judicial Police	:	300;
	Total number for one year	:	1500

3.10 In the case of *A v France*[31] heard by the European Court of Human Rights the accused was charged on 21 July 1981 with five other persons and a Mr Gehrling with attempted murder, infringement of the arms and ammunition legislation and infringement of legislation on the protection and control of nuclear substances. On the same day the investigating judge remanded Mrs A in custody, and the judge subsequently made an order finding that the six persons charged, including the applicant, had no case to answer, as there was insufficient evidence against them. In July or August 1980 Mr Gehrling went to the Paris police headquarters. He informed Chief Superintendent Aimée-Blanc, Head of the Central Office for the Prevention of Serious Crime, that Mrs A had hired him to kill Mr Pierre De Varga, who was himself facing charges in relation to the attempted murder of Prince Jean de Broglie. Mr Gehrling volunteered to make a telephonecall to Mrs A's home to discuss possible methods for carrying out the crime and to record the telephone conversation. Chief Superintendent Aimée-Blanc accepted Mr Gehrling's offer. Once the recording was in his possession, Chief Superintendent Aimée-Blanc informed his superiors of the threat to Mr De Varga, but did not reveal the identity of his informant or the existence of the cassette. When questioned on 22

---

31 Application no 14838/89.

September 1981 in connection with the investigation into the attempted murder of Mr De Varga, Chief Superintendent Aiméé-Blanc told the investigating judge that Gehrling called Mrs A from his office that he got her to talk about the case and that he recorded this conversation with a tape recorder which he kept. On 9 November 1981 Mrs A laid a complaint against Mr Gehrling and the Chief Superintendent for invasion of privacy and breach of the confidentiality of telephone communications. She relied on Articles 368, 369 and 378 of the Criminal Code and on Article L.42 of the Post and Telecommunications Code.

3.11 The European Court noted that three provisions of the French Criminal Code were relevant to the case:

- Article 368 "It is an offence punishable by a term of imprisonment of not less than two months and not more than one year and by a fine of not less than 2,000 francs and not more than 50,000 francs, or by one of the above penalties only, intentionally to interfere with the intimate side of another person's private life: (1) By intercepting, recording or transmitting with any kind of device words spoken in a private place by another person without that person's consent;
- Article 369 "It is an offence, punishable by the penalties set out in Article 368, knowingly to keep, to bring, or intentionally to allow to be brought, to the attention of the public or of a third person, or to use publicly or otherwise any recording or document obtained by means of one of the actions described in that Article.
- Article 378 ... any person who reveals secrets entrusted to him by reason of his status or profession, or of his temporary or permanent duties, except in those cases where he is obliged or authorised by law to lay an information, shall be liable to a term of imprisonment of not less than one month and not more than six months and to a fine of not less than 500 francs and not more than 15,000 francs. ..."

3.12 The Court noted that by its *Derrien* judgment of 13 June 1989, the Criminal Division of the Court of Cassation held that "although Articles 81 and 151 of the Code of Criminal Procedure permit an investigating judge to order, subject to certain conditions, the interception or recording of telephone conversations, no statutory provision authorises officers of the criminal investigation branch to carry out such operations in connection with a preliminary police inquiry", and that on 24 November 1989, the Court of Cassation declared void telephone tapping which had not been effected as part of a judicial investigation:

> It appears from the impugned judgment and the evidence produced in the proceedings that, having been informed that Christian Baribeau was engaged in drug-trafficking and had in particular had as a customer Andréé Salmeron, the police, on their own initiative, requested Salmeron to telephone Baribeau with a view to fixing a rendez-vous for a drugs delivery and recorded their conversation on cassette, then drew up a report on this operation; at the time fixed for the rendez-vous, the police were therefore able to follow Salmeron into Baribeau's home, arrest the occupants and proceed with a search;

> In order to refuse to annul the report describing the interception and recording of this conversation, the Court of Appeal held that the police had not used a technical device to intercept and record all the telephone conversations conducted from a subscriber's telephone; In making this ruling, when, without having obtained a warrant for this purpose from a judge, the police had, unknown to Baribeau, intercepted and recorded statements made by him on a telephone line which had been assigned to him, the Court of Appeal disregarded the above-mentioned provisions."

3.13 The European Court also considered Law no. 91-646 of 10 July 1991 which introduced a new Article 186-1:

> Any depository or agent of the public authorities, any agent of the public telecommunications operator or any agent of another operator of an authorised telecommunications network or of another provider of telecommunications services who, acting in the performance of his duties or on the occasion of the performance of his duties, has ordered, committed, or facilitated, in circumstances not covered by the cases provided for by law, the interception or diversion of communications issued, transmitted or received through telecommunications technology, or the use or disclosure of their content, shall be liable to a term of imprisonment of not less than three months and not more than five years and to a fine of not less than 5,000 francs and not more than 10,000 francs.

3.14 The European Court further noted article 9 of the Civil Code which provides as follows:

> Everyone has the right to respect for his private life. Judges may, without prejudice to a right to compensation for the damage sustained, order any measures, such as seizure, attachment and others, that may prevent or cause to cease an interference with the intimate side of private life; in the event of urgency such measures may be ordered on an interlocutory application.

3.15 Mrs A claimed that the recording of one of her telephone conversations had disregarded her right to respect for her private life and her correspondence, guaranteed under Article 8 of the Convention according to which everyone has the right to respect for his or her private and family life, home and correspondence and that there shall be no interference by a public authority with the exercise of this right except such as is 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 or morals, or for the protection of the rights and freedoms of others. The Court noted that Mrs A took the view that the recording of her telephone conversation with Mr Gehrling was incompatible with her right to respect for her private life and correspondence, guaranteed by Article 8.

3.16 The Government in substance contested the applicability of article 8. They maintained that there had been neither invasion of privacy nor interference by a public authority. On the first point, the Government drew attention to the fact that the recording in question had been made on the initiative and with the consent of one of the interlocutors. They argued further that the conversation intercepted had dealt exclusively and deliberately with matters - preparations of a criminal nature - which fell outside the scope of private life. As to the second, the Government affirmed that Mr Gehrling, who bore sole responsibility for instigating and carrying out the contested scheme, was not an official of the French State and was not acting on the latter's behalf. The fact that the public authorities had provided resources, such as premises and equipment, and had not opposed the undertaking in question was not sufficient to render them responsible for the interference.

3.17 The Commission and the applicant rejected this argument. They considered that a telephone conversation did not lose its private character solely because its content concerned or might concern the public interest. In addition, the recording was made on police premises with the assistance of a Chief Superintendent, who retained in his possession the relevant tape.

3.18 The Court observed that the undertaking complained of by the applicant depended on Mr Gehrling and Chief Superintendent Aiméé-Blanc working together and that they can hardly be dissociated from each other. The former played a decisive role in conceiving and putting into effect the plan to make the recording, by going to see the Chief Superintendent and then telephoning Mrs A. Chief Superintendent Aiméé-Blanc, for his part, was an official of a"public authority". He made a crucial contribution to executing the scheme by making available for a short time his office, his telephone and his tape recorder. The Court remarked that he admittedly, did not inform his superiors of his actions and he had not sought the prior authorisation of an investigating judge, but he was acting in the performance of his duties as a high-ranking police officer. The Court noted that it follows that the public authorities were involved to such an extent that the State's responsibility under the Convention was engaged, and the recording represented in any event an interference in respect of which the applicant was entitled to the protection of the French legal system. Furthermore, the interference in issue undoubtedly concerned Mrs A's right to respect for her "correspondence" - the Government did not dispute this. The Court was of the view that in these circumstances it was not necessary to consider whether it also affected her "private life". The Government conceded that the interference - if interference there had been - had not been "in accordance with the law". It had

not been consistent with the French law that had been in force at the material time (1980) because it had not been effected pursuant to a judicial procedure and had not been ordered by an investigating judge. The subsequent legislation - the Law of 10 July 1991 - made an interception of the type in question a punishable offence. Like the Commission, the Court noted that the contested recording had no basis in domestic law and it therefore found a breach of Article 8.

3.19 In *Lambert v France* the European Court of Human Rights remarked that when considering the necessity of interference, as it stated in its *Klass and Others v. Germany* judgment of 6 September 1978, the Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse, that this assessment has only a relative character as it depends on among other things the kind of remedy provided by the national law and it therefore has to be determined whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the interference resulting from the contested legislation to what is "necessary in a democratic society". The Court remarked as follows:

> The Court must accordingly ascertain whether an effective control was available to Mr Lambert to challenge the telephone tapping to which he had been made subject.
>
> 35. It notes, firstly, that the Court of Cassation in its judgment of 27 September 1993 held that the applicant had 'no *locus standi* to challenge the manner in which the duration of the monitoring of a third party's telephone line was extended' and that accordingly 'the grounds of appeal, which contest[ed] the grounds on which the Indictment Division [had] wrongly considered it must examine [the] objections of invalidity and subsequently dismissed them, [were] inadmissible'.
>
> 36. In its ruling the Court of Cassation therefore went beyond the ground relied on by the applicant concerning the extension of the duration of the telephone tapping and held that a victim of the tapping of a telephone line not his own has no standing to invoke the protection of national law or Article 8 of the Convention. It concluded that in the instant case the Indictment Division had been wrong to examine the objections of invalidity raised by the applicant as the telephone line being monitored had not been his own.
>
> ... [T]he provisions of the Law of 1991 governing telephone tapping satisfy the requirements of Article 8 of the Convention and those laid down in the *Kruslin* and *Huvig* judgments. However, it has to be recognised that the Court of Cassation's reasoning could lead to decisions whereby a very large number of people are deprived of the protection of the law, namely all those who have conversations on a telephone line other than their own. That would in practice render the protective machinery largely devoid of substance.
>
> 39. That was the case with the applicant, who did not enjoy the effective protection of national law, which does not make any distinction according to whose line is being tapped ...
>
> 40. The Court therefore considers, like the Commission, that the applicant did not have available to him the 'effective control' to which citizens are entitled under the rule of law and which would have been capable of restricting the interference in question to what was 'necessary in a democratic society'.

CHAPTER 4

THE LEGAL POSITION IN THE NETHERLANDS

4.1 Interceptions for security purposes are being performed by the *Binnelandse Veiligheidsdienst* (BVD). Interceptions may be authorised by the Prime Minister on application by the Minister of the Interior. A list of interceptions being performed must be submitted to a Council of Ministers for scrutiny every three months. Where crime is involved, monitoring of communications may be ordered by the investigating judge for the purpose of monitoring a suspect's communications. This is the case where the investigation urgently requires so and the suspicion relates to a serious offence for which an accused may be remanded in custody.

4.2 Monitoring is primarily aimed at obtaining evidence to be used in court, and the result of a "wiretap" may be used in evidence in the trial for the offence for which the wiretap was ordered. However, if the judge or police uncover other offences, the information concerning those offences may also be used as evidence when the other offences are tried in a subsequent trial. All investigating judges (*onderzoeksrechters*) are empowered to authorise the interception of communications. These judges are appointed from the ordinary corps of judges for a specific period in order to give guidance in respect of criminal investigations. The law does not set down a specific period for which a monitoring may be authorised, but in practice all authorisations are reconsidered after a period of four weeks. Extensions are also granted for periods of four weeks. The process is very informal. The investigation judge must be convinced that the authorisation should be extended. Interception or monitoring of communications may only be authorised if there is no less intrusive ways to investigate the case or obtain the evidence. In general it is accepted that monitoring is less intrusive than a physical search.

4.3 The following communications may be monitored or intercepted:

* Letters;
* Faxes;
* Data transmissions;
* E-mail, and in terms of a Bill still being considered, Internet;
* Telexes;

* Telephone conversations (including all types of mobile and cellular phones);
* Oral communications are in terms of the Bill, presently considered.

4.4 In practice, the prosecutor applies to the investigation judge for an authorisation to monitor communications. In a recent research report it was concluded that "wiretapping" is more frequently applied in the Netherlands than in Germany, the UK and the USA and that the interception of telephone communications is in practice felt to be a rather efficacious investigative method.[32]

4.5 A recent Telecommunications Bill privatises the telecommunications service providers. At present there are two mobile telephone operators, but it is expected that there will soon be more. Telecommunication service providers have to provide the means to monitor communications at their own costs. In terms of the Penal Code service providers commit contempt of court and are liable to imprisonment for a period of three months if they do not assist with the execution of a legal order. In extreme cases, the licence of a service provider may be revoked if he or she does not comply with an order for the monitoring of communications. The monitoring equipment used in duplicating an communication is the property of the service provider and a signal is duplicated and sent to the police for recording/monitoring. The legislation of the Netherlands complies with the guidelines of the European Court.

4.5 The subject of a security monitoring is never informed that his or her communications have been monitored. The person subjected to monitoring pursuant to an investigating judge's order, has to be informed of the monitoring if the disclosure will not jeopardise the investigation. There is presently a Telecommunications Bill before the First House of Parliament containing a general confidentiality clause which will protect the confidentiality of monitoring. Prisoners may be monitored if they are informed that the monitoring of communications are being done in specific areas of the prison. Bomb threats may be monitored without prior authorisation. Government employers or private employers may monitor state or business phones if they inform their employees beforehand that it will be done. Any person may record his own communications without the permission or knowledge of the other party.

---

32 Z Reine, RF Kouwenberg, MP Keizer *Tappen in Nederland*, The Hague, 1996, quoted in *Criminal Law*; Dr J A W Lensing, Kluwer Law International, The Hague, 1997, p 189.

4.6 Traffic data (call-related information) may be obtained even when interception or monitoring is not being done. A prosecutor has to apply to the investigation judge for authorisation to obtain such data. The following communications are privileged and may not be monitored, namely those of-

* A religious minister/priest and a member of the church;
* A medical practitioner and his or her patient.
* A lawyer and his client, unless they are both suspects in a crime.

4.7 The Telecommunications Bill[33] provides that private dwellings, vehicles, offices, etc. may be bugged. The process of control over recordings, sealing of such recordings, etc. are informal. Clause 13.1 of the Bill provides that telecommunication service providers may only provide such telecommunications services to their clients which are capable of being monitored (*aftapbaar zijn*). The Bill provides for rules to be made to determine the technical ability to monitor communications. Telecommunication network providers are obliged In terms of clause 13.2 to co-operate in the execution of a direction for the interception or monitoring of a communication. In the explanatory documents to the Bill the following is stated:

> "*De aanbieders van openbare telecommunicatienetwerken en openbare diensten tappen niet self af- dit is voorbehouden aan bevoegde instanties -maar faciliteren slechts het aftappen door op grond van wettelijke bepalingen tijdig organisatorische en technische maatregelen te treffen. Om te kunnen voldoenen aan deze wettelijke bepalingen moeten kosten gemaakt worden. Deze kosten vloeien dus voort uit wettelijke verplichtingen en hebben geen betrekking op het aftappen zelf. Vanuit dit oogpunt ligt het voor de hand dat deze kosten niet langer door de staat maar door de aanbieders gedragen worden*".

4.8 The reason for shifting the burden of the liability for the costs for the capability to intercept or monitor to the Service providers, is stated as follows: "*De staat wordt kortom gekonfronteerd met de gevolgen van de technische ontwikkelingen op het gebied van de telecommunicatie in de vorm van steeds hogere rekeningen voor de aftappen*". Certain costs will, however, still be borne by the state- the Ministry for the Interior will continue to pay costs relating to security investigations. The costs for the installation of monitoring rooms and the rental for the communications lines to the monitoring centres are being borne by the Ministry for the Interior and the Department of Justice. Other costs for which the state remains

---

33 Which was considered by Parliament during 1998.

responsible, are the administrative and personnel costs relating to a specific monitoring or request for call-relatedinformation. The Bill also grants the power to the Minister of Communications to extend the obligation to ensure the monitoring of communications to private persons or groups of persons.

CHAPTER 5

THE LEGAL POSITION IN BELGIUM

5.1 The monitoring of communications in Belgium is regulated by the "*wet van 30 juni 1994-ter bescherming van de persoonlijke levenssfeer tegen het afluistereren, kennisnemen en openen van privécommunicatie en telecommunicatie*". Private conversations and private telecommunications are addressed in the Act. In Belgium bugging of a private dwelling is only permissible with the authorisation of the owner or occupant of the dwelling. All communications which may be monitored in terms of the Belgium law must be recorded. The duration of an order for monitoring is one month and on expiration of the period it may be extended to six months. After six months a new application must be lodged. Each recording must mention the subject of the monitoring and the date of execution. In order to prevent misuse these particulars must automatically be mentioned with the recording, although it is not legally required. A warrant for a interception and monitoring may only be granted in cases of serious crime, namely terrorism, gang crimes (banditism), and organised crime. Monitoring, recording, listening to private communications and private telecommunications, except for the cases provided for by the law and authorised in terms of the law, are punishable as is the misuse or attempted misuse of a lawfully recorded monitoring. In cases of blackmailing or extortion the "Procureur des Konings" may order monitoring for a period not exceeding 24 hours, thereafter it has to be confirmed by an investigation judge ("onderzoeksrechter").

5.2 When the co-operation of the network operator is required for the execution of an order for monitoring, the investigation judge must issue two orders, namely one for the judicial police and one for the network operator. The network operator is only required to provide technical co-operation. The order to the judicial police must set out the date, the concrete facts of the case, the reasons for issuing the order, the subject of the order, the communications medium to be monitored, the location of any object which must be intercepted in terms of the order, and the period for which the interception and monitoring is authorised (which may not exceed one month), and the name and position of the officer of the judicial police to whom the order is addressed for execution. The order may be null and void if any of these particulars are omitted.

5.3 The network operator does not for security reasons receive the same detailed information. The order only provides the date of the order, the number of the subject and the

period for which the interception and monitoring is authorised to the network provider. Employees of the network operator are bound by secrecy. The investigation judge may only appoint an officer of the judicial police to execute the order and the officer may be assisted by agents of the judicial police. The names of these agents must be provided to the investigating judge beforehand. The officer responsible to execute the order must report in writing back to the investigation judge at least every five days. The officer concerned must hand over all recordings, transcriptions and translations to the investigation judge. The investigation judge decides which information is important for the investigation and he orders the drafting of a process verbal of the information. The order for monitoring, the process verbal and the five day reports of the investigation officer are filed in the investigation docket. When the monitoring is concluded, all information which has not been included in the investigation docket, is destroyed by the investigation judge and record is kept of such destruction. The recordings, the transcriptions and copies of the process verbal are sealed and kept by the "*griffie*" (master). The communications of doctors and advocates are privileged.

CHAPTER 6

THE LEGAL POSITION IN GERMANY

6.1 The European Union Standards, entitled "*Internationale Anforderungen für die rechtmässige Überwachung des Telekommunikationsverkehrs*", January 1995, are also applicable in Germany.

6.2 The catalogue of purposes for which and the crimes in respect of which interception may be used in Germany, are listed in the Code of Criminal Procedure in article 108 and includes criminal association, murder, manslaughter, currency related offences, robbery, extortion, drugs, treason, and espionage. The Secret Service and Customs are also permitted to use interception of communications in their investigations.

6.3 As a rule, an investigation judge may authorise the interception for a maximum period of 90 days. In an emergency, when a judge is not available, a prosecutor may authorise interception for a period of three days. Extension of the initial period of 90 days is only allowed with the submission of the successes obtained during the initial period. In practise, the police approaches the prosecution, after being authorised by a senior police official. The judge is then approached by the prosecution. It must be proved that monitoring is the last available investigation method or that other investigation methods have failed. Postal articles may be intercepted in terms of postal legislation. All telecommunications communications , namely fax, data, etc may be authorised to be monitored. Oral communications in offices dwellings, etc, may in future be intercepted in terms of a new law which came into operation on Saturday, 9 May 1998.[34]

6.4 Other rules apply to the Secret Service and Customs. Customs also have to obtain judicial authorisation for monitoring communications. The Intelligence Services have a parliamentary control body which consists of five senior political officials. Members of the Bundestag (Federal Parliament) exercises control over foreign intelligence surveillance.

6.5 All the service providers in the telecommunications market have been privatised since

---

34 Deutscher Bundestag Drucksache 13/8651 01.10.97.

1 January 1998. Deregulation was effected by the Telecommunications Act. All mobile phone network providers have been private from the outset. There are special provisions in the licensing agreements of the service providers which are regulated by the Telecommunications Act. All service providers must render assistance with the execution of monitoring orders. The service providers have to install all software and hardware to intercept or monitor telecommunications and the Police buy the recording equipment only. If service providers do not comply, their licences can be revoked.

6.6 Call-related information as old as 80 days can be obtained by the prosecution. The costs relating to interceptions are fixed by law. Investigators have the right to request call-related information from the service provider. The costs for a telecommunications line is 40 DM. The costs per call intercepted is paid by the Department of Justice. Manpower costs of the service provider as well as 125 DM per interception is payable.

6.7 All parties have to be informed by the prosecution of the interception after the conclusion of the interception, provided that follow-up investigations are not jeopardised by such communication. Two copies of the monitored communication are made, one is sealed for evidential (court purposes) and the other copy is used for investigation purposes. The only privileged communications are the communications between a lawyer and his client. Only the network operators are empowered to activate the monitoring.

CHAPTER 7

THE LEGAL POSITION IN BRITAIN[1]

7.1 The Interception of Communications Act of 1985 came into force on 10 April 1986.[2] Its objective was to provide a clear statutory framework within which the interception of communications on public systems would be authorized and controlled in a manner commanding public confidence.

7.2 A "public" telecommunications system is defined as a telecommunications system which is run pursuant to a licence granted under the Telecommunications Act 1984 and which has been designated as such by the Secretary of State.[3] Anyone who in terms of section 1(1) of the Act intentionally intercepts a communication in the course of its transmission by means of a public communications system is guilty of a criminal offence. Section 1(2) and (3) provides four circumstances in which a person who intercepts communications will not be guilty of the offence, namely:

* If the communication is intercepted in compliance with a warrant issued by the Secretary of State;
* If the person performing the interception has reasonable grounds to believe that the person to whom or from whom the communication is sent, has consented to the interception;
* If the communication is intercepted for purposes connected with the provision of postal or public telecommunications services or with the enforcement of any enactment relating to the use of those services;
* If the communication is being transmitted by wireless telegraphy and is intercepted, with the authority of the Secretary of State, for purposes of the issue of licences under the Wireless Telegraphy Act, 1949 or the prevention or detection of interference with wireless telegraphy.

---

1 See the *Halford* case, *supra*, p. 35 and further.

2 Interception of Communications in the United Kingdom February 1985, Cmnd 9438.

3 Section 10(1) of the 1985 Act.

7.3 Section 9 of the 1985 Act provides that no evidence shall be adduced by any party, in any proceedings before a court or tribunal, which lends to suggest either that an offence under section 1 of the 1985 Act has been committed by a public servant or that a warrant has been issued to such a person under section 2 of the 1985 Act. Sections 2 to 6 of the 1985 Act set out detailed rules for the issuing of warrants by the Secretary of State for the interception of communications and the disclosure of intercepted material. Section 2(2) of the 1985 Act provides as follows:

> "The Secretary of State shall not issue a warrant ... unless he considers that the warrant is necessary -
>
> (a) in the interests of national security;
> (b) for the purpose of preventing or detecting serious crime; or
> (c) for the purposes of safeguarding the economic well-being of the United Kingdom."

7.4 When considering whether it is necessary to issue a warrant, the Secretary of State must take into account whether the information which it is considered necessary to acquire could reasonably be acquired by other means[4] The warrant must specify the person who is authorized to do the interception, and give particulars of the communications to be intercepted, such as the premises from which the communications will be made and the names of the individuals concerned.[5] A warrant cannot be issued unless it is under the hand of the Secretary of State himself or, in an urgent case, under the hand of a senior official where the Secretary of State has expressly authorized the issue of the warrant. A warrant issued under the hand of the Secretary of State is valid for two months; one issued under the hand of an official is only valid for two working days. In defined circumstances, warrants may be modified or renewed.[6]

7.5 Section 6 of the Act provides, inter alia, for the limitation of the extent to which material obtained pursuant to a warrant may be disclosed, copied and retained. The Act also provides for the establishment of an Interception of Communications Tribunal. The tribunal consists of five members, each of whom must be a lawyer of not less than ten years' standing, who hold office for five years subject to re-appointment.[7]

---

4 Section 2(2) of the Act.

5 Sections 2(1) and 3 of the Act.

6 Sections 4 and 5 of the Act.

7 Section 7 of and Schedule 1 to the Act.

7.6 Any person who believes, inter alia, that communications made by or to him may have been intercepted in the course of their transmission by means of a public telecommunications system can apply to the tribunal for an investigation. If the application does not appear to the tribunal to be frivolous or vexatious, it is under a duty to determine whether a warrant has been issued, and if so, whether it was issued in accordance with the Act. In making this determination, the tribunal applies the principles applicable by a court on application for judicial review.[8]

7.7 If the tribunal determines that there has been no breach of the Act, it will inform the complainant, but it will not confirm whether there was no breach because there was no authorized interception or because, although there was such an interception, it was justified under the terms of the Act. In cases where the tribunal finds there has been a breach, it has a duty to make a report of its findings to the Prime Minister and a power to notify the complainant. It also has the power, inter alia, to order the quashing of the warrant and the payment of compensation to the complainant. The tribunal does not give reasons for its decisions and there is no appeal from a decision of the tribunal.[9]

7.8 The Act also makes provision for the appointment of a Commissioner by the Prime Minister. The first Commissioner was Lord Justice Lloyd (now Lord Lloyd), succeeded in 1992 by Lord Bingham, who was a senior member of the judiciary, and who was also succeeded in 1994 by a senior member, namely Lord Nolan.

7.9 The Commissioner's functions include reviewing the carrying out by the Secretary of State of the functions conferred on him by sections 2 to 5 of the 1985 Act, reporting to the Prime Minister breaches of sections 2 to 5 of the Act which have not been reported by the tribunal and making an annual report to the Prime Minister on the exercise of his functions. This report must be laid before Parliament, although the Prime Minister has the power to exclude any matter from it the publication of which would be prejudicial to national security, to the prevention or detection of serious crime or to the well-being of the United Kingdom. The report must state if any matter has been excluded.[10]

---

8 Section 7(2) to (4) of the Act.

9 Section 7(7) and (8) of the Act.

10 Section 8 of Act.

7.10 In general, the reports of the Commissioner to the Prime Minister have indicated an increase in new warrants issued, but the commissioner has been satisfied that in all cases those new warrants were justified under section 2 of the Act.

7.11 The English common law provides no remedy against interception of communications, since it places no general constraints upon invasions of privacy as such.

7.12 The Hong Kong Commission noted that in the United Kingdom the provisions of the Interception of Communications Act has been extended to the regulation of surveillance when conducted by the secret services. The Security Service Act 1989 applies to MI5 and the Intelligence Services Act 1994 applies to MI6. The Commission stated that the genesis of the 1989 Act was a ruling of the European Commission of Human Rights regarding complaints by office holders of the National Council for Civil Liberties (NCCL), an unincorporated association which works to monitor and defend civil and political rights in the United Kingdom. They explain that complaints arose from allegations that the office holders had been the subject of surveillance by MI5. The Hong Kong Commission pointed out that allegations were made by a former MI5 officer, in a television interview in 1985 and repeated in an affidavit sworn for the purposes of a judicial review, and, in line with government policy of not disclosing information about the operations of the Security Service, the United Kingdom neither confirmed nor denied the applicant's allegations.

7.13 The Hong Kong Commission pointed out that the European Commission noted that although the applicants *did* not allege that they were specific targets of telephone or mail intercepts, their evidence was that they had been subject to "indirect interception", i.e. the recording of information about them which appeared in the telephone or mail intercepts of targets. They further remarked that the Commission found that there was a reasonable likelihood that the applicants were the subject of secret surveillance and it therefore had to consider whether such interference was "in accordance with the law". The Hong Kong Commission explained that the Commission applied the *Malone* test of a law which is sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which surveillance may apply, that the Commission noted that the Security Service exists for the exclusive purpose of the defence of the Realm and that the Security Service's activities were governed by a Directive, but not authorised by law:

> "Members of the Security Service are public officials but unlike, for example, police officers, immigration officers or officers of HM Customs and Excise, they have conferred on them not special powers whether under any law or by virtue of the Directive. Although the Directive is published, it is not claimed by the Government that it has the force of law or that its contents constitute legally enforceable rules concerning the operation of the Security Service. Nor does the Directive provide a framework which indicates with the requisite degree of certainty the scope and manner of the exercise of discretion by the authorities in the carrying out of secret surveillance activities."

7.14 The Hong Kong Commission noted that the Commission accordingly found that there had been a violation of article 8 of the European Convention because the surveillance was carried out by a body which had no legal authority, and therefore was not authorised by law. They further pointed out that the legislation was introduced anticipating an adverse ruling to similar effect by the European Court and that MI6, the security service concentrating on foreign intelligence, and the Government Communications Headquarters was also now put on a statutory footing under the Intelligence Services Act 1994. The Hong Kong Commission remarked that that Act also establishes a system of parliamentary accountability of both these services and MI5 and that section 1 of the Security Service Act 1989 sets out the function of the Service (i.e. MI5) as follows:

> "[It] shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. ...
>
> It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands. "

7.16 The Hong Kong Commission considered that this explication, if not an exhaustive definition, of "national security" is useful, in view of former United States Attorney General Griffen Bell's comment that "national security" has become a "talismanic phrase" which has been used "to ward off any questions about the legitimacy of any governmental conduct to which the phrase was applied." The Commission noted that the general structure of the legislation is similar to that of the Interception of Communications Act and the main components are a warrant system to authorise intrusions, provision for their renewal or cancellation, the appointment of a senior judge as Commissioner, and the establishment of a tribunal to consider complaints. They also pointed out that section 3 of the 1989 Act provides that "no entry on or interference with property shall be unlawful if it is authorised by a warrant". The Hong Kong

Commission emphasised that section 5 of the 1994 Act is wider and provides that a warrant can authorise any of the three secret services (MI5, MI6, and Government Communications Headquarters) to interfere with property, trespass on land or interfere with wireless transmissions.

CHAPTER 8

THE LEGAL POSITION IN THE UNITED STATES OF AMERICA

8.1 The Foreign Intelligence Surveillance Act (FISA) established procedures for judicial regulation of surveillance activities undertaken in the furtherance of national security interests.[11] The Foreign Intelligence Surveillance Court (FISC) is established In terms of article 1803 of the Act. Seven circuit court judges are designated by the Chief Justice to hear applications for and pass judgment on foreign intelligence surveillance orders. An appellate level court, comprised of both district and circuit court judges appointed by the Chief Justice, which review denials of FISA applications is also established in terms of the Act. Judges at both levels may sit for up to seven years, and may not be reappointed. Denials at the appellate level may be appealed to the Supreme Court.

8.2 A federal officer may, with the Attorney-General's approval apply to a FISC judge for a court order to conduct FISA surveillance. Such an order is valid for ninety days. Guidelines which regulate the use of information gained by FISA surveillance are provided for in section 1807 (a)-(d) of the Act.

8.3 The Act provides for judicial authorization to do electronic surveillance in respect of the international communications of United States citizens and resident aliens, and protects such communication from eavesdropping without court order regardless of where the surveillance is conducted. By definition, electronic surveillance is the acquisition by means of surveillance devices of any wire or radio communication sent or received by a United States person (including both a citizen or resident alien) in which that person has a reasonable expectancy of privacy.

8.4 The privacy expectation requirement excludes commercial broadcasts, home radios and citizen band broadcasts. Section 1801 (f)(4) includes oral communication, and the installation of beepers and television cameras. This paragraph is inapplicable in consent surveillance situations, as no right of privacy exists in such circumstances. FISA does not regulate the use

---

11 See detailed discussion of intelligence surveillance in Carr, James G. *The Law of Electronic Surveillance*. New York, 1986 2nd Edition 9-6, - 9-9.

of a body microphone by a consenting informant.

8.5 The Act only applies if the surveillance is intended to acquire "foreign intelligence information", of which there is five definitions: "the first three definitions include information which relates to, and, if concerning a United States person, is necessary to the ability of the United States to protect against: (1) actual or potential attack, (2) sabotage or terrorism, or (3) clandestine intelligence activities. Actual or potential attack encompasses information regarding foreign military strength and intentions. Clandestine intelligence activities includes 'classic counter intelligence information', but not, for example, information related to political activity within the United States by United States persons or to information necessary to ascertain the degree of involvement in such groups by foreign powers."[12]

8.6 Other interests included in the definition are security and national defence, and the conduct of the foreign affairs of the United States. It is, however, required that there must be a direct relation to a United States person's activities on behalf of a foreign power. A foreign power or agent thereof includes foreign embassies and counsellors as well as other "official foreign government establishments." It could also include different factions of foreign nations which are foreign based and controlled. International terrorist groups are also included in the definition.

8.6 Under section 2516 of Title III of the *Omnibus Crime Control and Safe Streets Act* of 1968, now codified as 18 U.S.C. §§ 2510-20 of 1994, the Attorney-General, Deputy Attorney-General, Associate Attorney-General, or any assistant Attorney-General specially designated by the Attorney-General, may authorize an application to a federal judge of competent jurisdiction for, and such judge may grant an order authorizing or approving the interception of wire or oral communications by the Federal Bureau for Investigation, a Federal Agency having responsibility for the investigation of the offence as to which the application is made, when such interception may provide or has provided evidence of -

- any offence punishable by death or by imprisonment for more than one year, offences relating to the enforcement of the Atomic Energy Act, 1954, or relating to espionage, sabotage, treason or riots;

---

12 Carr *supra* p. 9-8.

- any offence involving murder, kidnapping, robbery or extortion;
- bribery of public officials and witnesses, bribery in sporting contests, unlawful use of explosives;
- influencing or injuring an officer, juror or witness, obstruction of criminal investigations or obstruction of law enforcement;
- presidential and presidential staff assassination or kidnapping;
- racketeering;
- sexual exploitation of children;
- counterfeiting and fraud;
- drug offences;
- any conspiracy to commit any of the above offences.

8.8 The procedure for obtaining an order for interception is prescribed in article 2518. All such applications must be made in writing upon oath or affirmation. Upon such application, the judge may enter an ex parte order, authorizing or approving interception of wire or oral communications within the territorial jurisdiction of the court in which the judge is sitting, if the judge determined on the basis of the facts submitted to him that -

(a) there is probable cause to belief that an individual is committing, have committed or is about to commit a particular offence enumerated in the Act;

(b) there is probable cause for belief that particular communications concerning that offence will be obtained through such interception;

(c) normal investigative methods have been tried and have failed or reasonably appear to be unlikely to succeed if tried, or too dangerous;

(d) there is reasonable cause to belief that the facilities from which, or the place where, the wire or oral communication are to be intercepted, are being used, or are about to be used in connection with the commission of such offence, or are leased to, listed in the name of, or commonly used by such person:

8.10 The judge may direct that a communication common carrier, landlord, custodian or other person must furnish the applicant of the order forthwith with all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference. Any services rendered in this regard must be compensated.

8.11 The order may not authorize interception for a period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days. Extensions of the order may be granted on application made in the same manner as the initial order, for a further maximum period of 30 days at a time. The order may require reports to the judge on the execution thereof.

8.12 There is provision for interception without an order in emergency situations, namely if an emergency exists that involves -

(a) immediate danger of death or serious physical injury to any person;
(b) conspirational activities threatening the national security interest; or
(c) conspirational activities characteristic of organized crime.

8.13 A proper application must, however, be made within 48 hours after the interception has occurred, or begins to occur. Such interception must immediately terminate when the communication sought is obtained, or when the application is denied, whichever is earlier.

8.14 Section 2511 of Title III punishes the wilful interception of wire and electronic communications, the wilful use of intercepting devices already installed and the wilful disclosure or use of the content of intercepted communication by any person knowing or having reason to know that the information in question has been thus obtained, each of which amounts to an independent offence with not more than five years imprisonment or a fine or both.

8.15 Evidence acquired in violation of the relevant legislation (unauthorized interception) are inadmissible in any trial, hearing or other proceedings.[13]

8.16 The Communications Assistance for Law Enforcement Act (CALEA) was adopted, inter alia, to regulate the obligations of telecommunications service providers.[14] The law also sets out the requirements for the surveillance of wire or electronic communications in regard to law enforcers. The primary purpose of the CALEA is to clarify a telecommunications carrier's duty to assist law enforcement agencies with the lawful interception of communications and the

---

13 Section 2515 Title III.

14 Public Law 103-414; 47 U.S.C. 1001-1010.

acquisition of call-identifying information. To ensure that law enforcement agencies can continue to conduct authorized surveillance of wire or electronic communications, the CALEA states that telecommunications carriers must meet the assistance capability requirements set forth in section 103 of the Act. Section 104 of the CALEA mandates the Attorney-General of the United States to provide notice of estimates for the actual and maximum number of pen register, trap and trace and communication intercepts that law enforcement agencies may use simultaneously.

8.17 The capacity requirements are not intended to specify, require or prohibit adoption of any particular system, design or configuration by a telecommunications carrier, equipment manufacturer, or support services provider. These entities must develop an appropriate solution to comply with the capacity requirements set forth in a notice issued in terms of section 103. A fine of $10 000 per day for non-compliance with the Act may be levied.[15]

8.18 The Hong Kong Commission noted in regard to the CALEA that concerns were raised about security, the impact on the role of service carriers and the cost incurred by telephone companies. The Commission noted that a criticism levelled against the CALEA is that the effect of the legislation would be to assist eavesdropping by law enforcement agencies, but it would also apply to users who acquire the new technology capability and make it easier for criminals, terrorists, foreign intelligence (spies) and computer hackers to electronically penetrate the phone network and pry into areas previously not open to snooping. The Commission pointed out that it is hence suggested that this situation of easier access due to new technology changes could therefore affect national security. The Hong Kong Commission also remarked that the President of the United States Telephone Association has criticised the legislation's potential impact on the role of service carriers. They stated that he noted the co-operative working relationship that exists between telephone companies and law enforcement, and that he said that such legislation forces local exchange carriers to become, in effect, agents of the law enforcement community, rather than maintaining the more appropriate arms-length relationship between common carriers and law enforcement. The Hong Kong Commission further noted that also of concern are the costs incurred by telephone companies for necessary technical conversions of their switches and computers which has been estimated at between

---

15 For a more detailed discussion regarding the CALEA, see Dorothy E. Denning "Denning to tap" Georgetown University "*Comm. Of the ACM*, Vol 36 No. 3. March 1993. 24-33.

US$500 million and US$1.8 billion and that the legislation requires the government to reimburse the telephone companies. They pointed out also that the public may intervene in proceedings before the Federal Communications Commission concerning telephone companies' measures to alter their technology and resultant costs.

8.19 Dr Duncan Chappell noted that more than $ 500 million (US) was budgeted by Congress to pay for the cost of adopting new technology to meet interception capabilities.[16] He pointed out that procedures were also established for the issue by the Federal Attorney General of a notice of future capacity of intercept requirements to the communications industry within one year of CALEA's enactment. He remarked that the FBI acting under the delegated authority of the Attorney General issued such a notice in October 1995 which was, however, later withdrawn as a result of widespread public criticism and a new notice was issued in January 1997. Dr Chappell stated that the latter notice called for a substantial increase in surveillance both of landline and wireless communications over the next 10 years with a total maximum capacity of more than 57 000 simultaneous intercepts to be conducted in the United States. He noted that this notice was rejected by industry and privacy groups alike for proposing an even greater capacity for interceptions by carriers than was currently required at a prohibitive cost. Dr Chappell noted that critics urged that the deadline for compliance with CALEA's provisions which was set for October 1998 should be extended to October 2000 in order to permit more rigorous review of the FBI's proposals before setting industry interception capability standards. He pointed out that this extension seemed likely to be granted.

8.20 Dr Chappell stated that the debate over encryption has pitted computer industry and civil liberty groups against law enforcement and intelligence agencies. He considered that this debate is not only central to the maintenance and growth of trade and commerce, and to privacy protection, but also to the ability of law enforcement and national security bodies to understand what they are still able to intercept. He noted that the FBI has been lobbying actively on behalf of the law enforcement community to limit or prevent the use of encryption in the United States and its export abroad. He explained that a concerted effort has been made to require manufacturers and users of encryption to lodge in escrow with independent authorities the special key needed to unlock and make intelligible encoded data, and that the

---

16 "Law Enforcement Co-operation: The Interception of Communications and the Right to Privacy" at 23.

so-called key escrow system would allow law enforcement agencies in the United States or elsewhere to gain access to a key to crack a code in the course of a criminal investigation. Dr Chappell further remarked that critics of the key escrow proposal have suggested that it poses a serious threat to privacy since there is a danger that access keys could be abused by law enforcement agencies and others, and that it would also require the United States and other democratic countries to share escrow information with law enforcement agencies in countries with poor human rights records.

8.21 The Hong Kong Commission noted that a different approach has been adopted in Australia in regard to the tappability of communications. They pointed out that in 1990 the Australian Cabinet determined that all public telecommunications services should be capable of being intercepted for law enforcement and national security purposes and in 1991 licence declarations were amended to require that a licensee must not operate a telecommunication network unless:

* it is possible to execute a warrant under the Telecommunications (Interception) Act 1979 in relation to a telecommunications service provided by that network; or
* if it is not possible to execute such a warrant (there being no legislative constraint on the manufacture and use of encryption devices in Australia), the Minister, after consultation with the Attorney General, authorises the licensee's operation. Authorisations have been issued under this provision.

8.22 The Hong Kong Commission remarked that notwithstanding this legal framework, the Australian Barrett Report specifically rejects legislation along United States lines imposing a unilateral requirement that carriers/service providers only introduce technology that is interceptable, and that it reasoned that "such a unilateral policy runs the risk of implementing less than world class technology which could put Australia at a major disadvantage in a cost sense", but, "the sooner an *international* requirement for interception is standardised and accepted, the more likely there will be the automatic provision of TI capability in new technology with similar implications for all users". They noted that the Barrett report expected it to take 3 to 8 years for such an international agreement to be reached.

8.23 It has been testified before US Senate hearings that "Evidence gathered through

electronic surveillance .... has had a devastating effect on organized crime." According to the Federal Bureau for Investigations (the FBI), the hierarchy of organized crime has been neutralized or destabilized through the use of electronic surveillance, and thirty odd years of successes would be reversed if the ability to conduct court-authorized electronic surveillance was lost.[17] Hence, there is no doubt that the FBI regards electronic surveillance as the cornerstone of organized crime and racketeering investigations.

8.24 Almost two-thirds of all court orders for electronic surveillance are used to fight the war against drugs, and electronic surveillance has been critical in identifying and dismantling major drug trafficking organizations. The use of electronic surveillance has successfully prevented several terrorist attacks. It is also a less dangerous investigation method and is critical in those situations where the crime leaders are not present at the places where the illegal transactions take place, as is the case with major drug cartels directed by distant drug chieftains. For the first time, investigators in the United States are now allowed to eavesdrop on alien smuggling plans by monitoring telephone conversations. Through electronic surveillance, federal agents learned that the operations were as sophisticated as drug cartels. US Attorney, Alan Bersin is quoted as having said: "The use of wiretaps gives us the ability to go up the food chain and start to take down the heads of these organizations." In 1997, 1186 wiretaps requests were authorized for a total of 2,5 million intercepted conversations.[18]

---

17 Denning, *supra* p. 28.

18 *Global Crime Update* No. 18 - May 29 1998 p. 2.

CHAPTER 9

THE LEGAL POSITION IN HONG KONG

A. Background

9.1 As was noted in the preceding chapters the Law Reform Commission of Hong Kong considered the issue of regulating surveillance and the interception of communications recently.[19] This investigation resulted in the Interceptions of Communications Ordinance which has not yet, however, been put into operation.

B. The need for requiring authorisation for surveillance and interception by warrant

9.2 The Hong Kong Commission considered, inter alia, whether all surveillance and interception of communications should require authorisation by warrant.[20] The Commission noted that a warrant system is essential where the authority cannot effect the intrusion without technical assistance, for instance, by the telecommunication service provider and/or where the activity in question is likely to be challenged, such as physical entry to premises. They considered that from a strictly pragmatic perspective, a warrant system is less necessary where the intrusion can be effected surreptitiously and without outside assistance. They remarked that under the Personal Data (Privacy) Ordinance exceptions are self-executing, but reviewable, and under its system, the exception is invoked by the data user on the basis that the terms of the statutory exemption apply, but this is subject to challenge by the data subject, and will then be reviewed by a supervisory authority. The Hong Kong Commission considered that while this system should suffice in dealing with departures from the data protection principles, they considered it inadequate in sanctioning the more serious intrusions entailed by surveillance and the interception of communications. The Commission said that in addition, use of exemptions under the Personal Data (Privacy) Ordinance is more transparent - data subjects will become aware of refusals of access and many changes of use. By way of contrast, an individual will seldom become aware of being made the subject of surveillance or interceptions. The Hong

---

19 See Law Reform Commission of Hong Kong *Privacy: Regulating Surveillance and the Interception of Communications* Consultation Paper 1996 at http://www.info.gov.hk/info/pricon.htm accessed on 5/11/1998.

20 *Privacy: Regulating Surveillance and the Interception of Communications.*

Kong Commission noted that the alternative is a warrant system and that this is the conventional mechanism adopted by, for instance, the United Kingdom legislation in sanctioning intrusion to property and interception of communications. The Commission considered that the warrant system has two advantages; firstly, it entails approval by an independent authority prior to the intrusion being undertaken, and, secondly, it furnishes the intruder with a written authority which he can produce if challenged. They noted that this second advantage is a practical necessity where the intrusion in question either-

* required the technical assistance of a third party. (This is the usual position when intercepting public telecommunications systems. While it is theoretically possible for a law enforcement agency to unilaterally hack into the public telecommunications switching programs and effect taps, it is much simpler and surer to approach the public telecommunications company and request that they arrange matters); or
* the intrusion is of a nature which carries the risk of being detected by the victim. (This is the case where physical intrusion into premises is involved).

9.3 The Hong Kong Commission noted that in the United Kingdom all intrusions regulated by law (and hence the warrant requirement) fall into one or other of these categories. They stated that their recommendations however propose much more comprehensive regulation of surveillance, whether or not interceptions or physical intrusion are involved. The Commission remarked that the issue therefore arises whether a warrant should also be required in those situations where the intrusion requires no external assistance and is inherently undetectable, noting that most remote surveillance falls into this category.

9.4 The Hong Kong Commission concluded that a warrant requirement should extend to this latter situation also, so that it would apply to all proscribed surveillance and interception activities and that a warrant procedure is merited in view of the seriousness of all such intrusions. They considered furthermore that to subject only some intrusions to the warrant procedure would encourage snoops to turn to surveillance and interception activities that fell outside that requirement.

C. Who should issue warrants?

9.5 The Hong Kong Commission noted that the authority to authorise the warrant is in the United Kingdom a government Minister, whereas in the United States it is a court, in Australia a court deals with law enforcement warrants and the Attorney General deals with security-related warrants. They noted the following comment on the issue of warrants being authorised by a government minister, rather than a judge-

> "[it] may seem anomalous for several reasons: interception is analogous to search, for which warrants are issued by the judiciary (when required in law) and it offends conceptions of the rule of law and separation of powers for a minister of the crown to authorise interception by another part of the executive. It fails to provide an independent check on the power to prevent potential political abuse. While there may be a strong case for implementing the recommendation of the Royal Commission on Criminal Procedure that interception warrants should be issued by magistrates in criminal investigations, whether those arguments apply with equal force in the domain of security investigations is more doubtful. Certainly it may be said that the nature of the evidence supporting the application will be different in the two types of case. In these circumstances a minister may, because of access to background information, have a fuller picture than a magistrate or a judge of the overall intelligence significance of the proposed surveillance . . . In view of the fact that the process will of necessity exclude the targeted person from making representations prior to interception, it seems essential to require the authorities to satisfy an outsider of the need for it. We would, therefore, favour the introduction of a greater independent element (though not necessarily judicial control) prior to interception occurring."

9.6 The Hong Kong Commission remarked that their courts already grapple with security issues in dealing with public interest immunity certificates in criminal trials. They noted that in the United Kingdom, judges perform the roles of Commissioner for Interceptions and Commissioner for the Security Service. They pointed out that this issue was addressed in *US v United District Court* where the United States Government submitted that the courts were not equipped to assess security matters which was as follows unanimously rejected by the Supreme Court:

> "We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. ... There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. ... If the threat is too subtle or complex for our senior enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance."

9.7 The Hong Kong Commission was of the opinion that the additional independence afforded by a judicial determination is necessary in Hong Kong. They noted that section 44(2)

of the Personal Data (Privacy) Ordinance provides that prior to obtaining the identification of journalistic sources, the Privacy Commissioner must obtain the approval of the High Court. They thought that this should similarly be the case in Hong Kong in the authorisation of warrants sanctioning intrusions, whether the public interest invoked relates to law enforcement or to security. They remarked that it is important that friction be avoided between the judiciary and the executive and that dividing-up the issuing of warrants according to whether they relate to crime (for the judiciary) or security (for the executive) would be difficult. The Commission pointed out that the advantage of having a judge scrutinise all applications is that it ensures that those applying for the warrant will have to think the matter through, it diminishes the prospect of abuse of power and it is also reassuring to the public. They further noted that restricting the power to the High Court should also make for greater consistency of approach. The Commission consequently recommended that all applications for warrants for surveillance or interception should be made to the High Court.

9.8 The Interceptions of Communications Ordinance provides as follows on the authority who should issue warrants who may make applications for interception of communications and the particulars to be contained in the applications:

> 4(1) Subject to the provisions of this section, a judge of the High Court may make a court order authorizing a person named in the order to intercept, in the course of its transmission by the post or by means of a telecommunication system, such communication as are described in the order.
>
> 5(1) An application to the High Court for an order authorizing the interception of communications under section 4 may only be made by-
>
> (a) any officer of any officer of the Royal Hong Kong Police Force of or above the level of superintendent;
>
> (b) any senior officer of the Customs and Excise Service as defined in section 2 of the Customs and Excise Service Ordinance (Cap 342);
>
> (c) any investigating officer authorized by the Commissioner of the Independent Commission Against Corruption and who is appointed under section 8 of the Independent Commission Against Corruption Ordinance (Cap 204);
>
> (d) any senior officer of the Immigration Department; or
>
> (e) any senior officer of the Correctional Services Department.
>
> (2) An application for authorization shall be made ex parte and in writing to a judge of the High Court in Chambers and shall be accompanied by a sworn affidavit deposing to the following matters-
>
> (a) the name and rank of the officer making the application;
>
> (b) particulars of the offence or offences under investigation;
>
> (c) the name and address of the person who is believed to have committed, is committing or is about to commit the offence or offences under paragraph (b) and whose communications are to be intercepted for the purpose of investigating that offence;

(d) a description of the nature and location of the facilities from which or the place where the communication is to be intercepted;
(e) the type of communication sought to be intercepted and the method of interception to be used;
(f) whether he wishes for a person authorized under the Post Office Ordinance (Cap 98) or the Telecommunication Ordinance (Cap 106) to assist him with the interception;
(g) what other investigative methods have been used and why they have failed or are unlikely to succeed;
(h) the duration of the interception; and
(i) particulars of any previous application involving the same person.

9.9 The Hong Kong Commission was of the view that the judge's consideration of a security-related warrant would entail his or her making an independent assessment of the factual issues. They remarked that it would require that the judge should be satisfied that authorisation is warranted on the basis of the broad picture deposed to by relevant officials. They explained that, for example, the affidavit may state that as a result of information received, it was reasonably believed that a terrorist attack was imminent. They envisaged that as with other *ex-parte* warrants, they would usually be dealt with on paper and a hearing would seldom be required. The Commission stated that the issue of closed hearings does not arise and that the duty judge system will provide 24 hour access. They were of the view regarding emergency taps, such as in hostage or other life-threatening situations that such interceptions should be subsequently ratified by judicial authorisation. They recognised the impracticability in such circumstances for an application to be made to a judge in every case before interceptions to be initiated, but noted also that dispensing with a system of *ex post facto* authorisation could seriously undermine the safeguard of judicial scrutiny. The Hong Kong Commission therefore recommended that in circumstances where it is impractical because of the urgency of the situation (as where life is at risk) to obtain approval from the court before initiating an interception, it should be permissible to apply to the court *ex post facto* for a warrant.

9.10 The following provisions were included in the Interception of Communications Ordinance to govern the position of urgent applications:

> (3) Where a serious threat of death or bodily harm to a person exists and it is impracticable to make an application for an order authorizing the interception of communications in accordance with subsection (2), an officer listed in subsection (1), with the written permission of-
> (a) the Commissioner of Police, where the officer involved is an officer of the Royal Hong Kong Police Force;
> (b) the Commissioner for Customs and Excise Service, where the officer involved

is a senior officer of the Customs and Excise Service;

(c) the Commissioner of the Independent Commission Against Corruption, where the officer is an officer of the Independent Commission Against Corruption;

(d) the Director of Immigration, where the officer is an officer of the Immigration Department; or

(e) the Commissioner of Correctional Services, where the officer is an officer of the Correctional Services Department,

may intercept a communication without prior authorization.

(4) Where an interception under subsection (3) occurs, unless the officer conducting the interception makes an application for authorization in accordance with subsections (1) and (2) within 48 hours from the beginning of the interception giving-

(a) the reasons for not making an application prior to interception; and

(b) a copy of the written permission given by-

(i) the Commissioner of Police, where the officer involved is an officer of the Royal Hong Kong Police Force;

(ii) the Commissioner for Customs and Excise Service, where the officer involved is an officer of the Customs and Excise Service;

(iii) the Commissioner of the Independent Commission Against Corruption, where the officer involved is an officer of the Independent Commission Against Corruption;

(iv) the Director of Immigration, where the officer is an officer of the Immigration Department; or

(v) the Commissioner of Correctional Services, where the officer is an officer of the Correctional Services Department,

the interception shall be deemed unlawful under section 3.

(5) Any interception which is conducted pursuant to subsection (3) shall immediately terminate when the communication sought is obtained or when an application for authorization is denied, whichever is earlier.

(6) Where an application for authorization under subsection (4) is denied, the intercepted material shall be destroyed immediately.

D. Private sector intrusions

9.11 The Hong Kong Commission notes that in other jurisdictions the warrant system envisages the approval of intrusions by public authorities. They consider that in principle, in some situations private agencies may be able to make out a case why their surveillance/interception activities would further one of the public interests they have identified as justifying intrusion, such as the prevention or detection of serious crime. They state that for example, companies that wish to avoid the embarrassment of a police investigation often hire private investigators to investigate offences. They therefore recommended that authorisation by warrant should be available to sanction intrusions by both public authorities and private companies but that private sector applicants should have to satisfy a more stringent public interest test. As was noted above section which was included in the Interception of Communications Ordinance does not make provision for private individuals applying for orders

authorizing the interception of communications.

E. Criteria for interception

9.12 The Hong Kong Commission examined the scope of public interest justifications for intrusions which would otherwise contravene the offences they have defined prohibiting surveillance and/or the interception of communications.[21] The Commission remarked that in formulating these public interest grounds justifying the issue of a warrant they have endeavoured to heed the proposal that they constitute "precise and rigorous criteria ... subject to careful and effective scrutiny after the event." The Commission noted that "security, defence and international relations in respect of Hong Kong" is the phrase used in the Commissioner for Administrative Complaints Ordinance (Cap 397) and which was subsequently adopted in the Personal Data (Privacy) Ordinance. They considered that the test should be along the lines that the information would be of substantial value in safeguarding security, defence, and international relations. The Commission further noted that the United Kingdom Interception of Communications Act 1985 provides that a warrant may be issued where the intrusion is for the purpose of "preventing or detecting serious crime." They pointed out that "serious crime" is defined by section 10(3) of the UK Interception of Communications Act as follows:

> "(a) it involves the use of violence, results in substantial financial gain or is conducted by a large number of persons in pursuit of a common purpose; or
>
> (b) the offence or one of the offences is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three

---

21 The Hong Kong Commission recommended the control of surveillance comprising the following three criminal offences:

- entering private premises as a trespasser with intent to observe, overhear or obtain personal information therein;
- placing, using or servicing in, or removing from, private premises a sense-enhancing, transmitting or recording device without the consent of the lawful occupier;
- placing or using a sense-enhancing, transmitting or recording device outside private premises with the intention of monitoring either the activities of the occupant or data held on the premises relating directly or indirectly to the occupant without the consent of the lawful occupier.

The Commission stated that "private premises" in this context means any private residence, together with its immediate curtilage (garden and outbuildings), but excluding any adjacent fields or parkland, and that it should in addition cover hotel bedrooms (but not other areas in a hotel) and those parts of a hospital or nursing home where patients are treated or accommodated; school premises; and commercial premises, aircraft, vessels and vehicles from which the public are excluded.

years or more."

9.13 The Hong Kong Commission noted in regard to this provision that while (b) is definite enough, (a) has been criticised for its vagueness since it is not at all clear how many people would constitute "a large number of persons". They considered, however, that it seems that many public order offences would be covered by the provision. They pointed out that it will be recalled that in the *Malone* case the European Court held that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances" in which tapping will be authorised. The Commission also referred to the comparable provision in the Australian Telecommunications (Interception) Act 1979, stating that it is both more restrictive and specific, with a criterion of seven years imprisonment. They pointed out that the Barrett Review has recommended that this be reduced to three years, provided it also involves "... two or more offenders and substantial planning and organisation; involves the use of sophisticated methods and techniques; and is of a kind ordinarily committed in conjunction with other like offences."

9.14 The Hong Kong Commission stated as these above-mentioned provisions indicate, the difficulty is in identifying the cut-off point distinguishing "serious" crime from other crime. They noted, however, that the United Kingdom provision does not refer to the maximum sentence, but to the tariff that is likely to be imposed in the particular case and that this would usually be much less than the maximum prescribed. The Hong Kong Commission concluded that an offence punishable by a minimum of seven years imprisonment would adequately reflect the gravity of the offences they believed should justify the issue of a warrant. They accepted, however, that some offences which do not attract sentences at that level may nevertheless be considered by the community to pose such a threat to the fabric of society that they should fall within the scope of "serious crime" for the purposes of their surveillance and interception proposals. They therefore recommended that "serious crime" should mean either an offence punishable by at least seven years imprisonment, or an offence punishable by at least three years imprisonment where there is an element of bribery or corruption. They also acknowledged that there may be categories of offence other than bribery or corruption which respondents to their Consultation Paper may wish to add.

9.15 The Hong Kong Commission also pointed out that the United Kingdom provision extends to the "prevention or detection" but not the "prosecution" of crime. They noted that the words

"preventing or detecting such crime", and the significance of this omission were considered by the House of Lords in *R v Preston* where five defendants were charged with importing drugs and sought access to prosecution evidence of intercepted conversations. The Commission stated that the defendants hoped that that evidence would establish duress and/or their innocence and that the trial judge refused the defendants' request that they be provided with the transcripts, but nonetheless admitted them as evidence. They noted that the House of Lords held that "the prevention or detection of crime" did *not* extend to the *prosecution* of the offence and that the conclusion also accorded with the stringent limitations on the retention of intercepted data:

> "To my mind the expression 'preventing and detecting' calls up only two stages of the fight against crime. First, the forestalling of potential crimes which have not yet been committed. Second, the seeking out of crimes, not so forestalled, which have already been committed. There, as it seems to me, the purpose comes to an end. I accept that the successful prosecution of one crime may in a sense prevent another, either because it puts the particular offender out of circulation for a while, or because the fact of conviction in respect of one crime may deter the commission of others. But although prevention in this sense may be a by-product of a prosecution, the word seems a very odd choice if the purpose of the interception was to reach forward right up to the moment of a verdict."

9.16 The Hong Kong Commission considered that the essential policy question is whether it is right that intrusions should only be legally sanctioned at the investigative stage. They agreed with the United Kingdom approach whereby intrusions should only be lawful up to, but not including, the prosecution of an offence, since otherwise the prosecution would be able to continually refine its charges up to the date of the trial. The Commission considered that in practical terms the cut-off point between prevention/detection and prosecution is the laying of the charge and the police admittedly have considerable discretion as to the timing of this. They remarked that such a restriction would also accord with the position whereby a suspect is not further interviewed once he has been charged and also with solicitor-client confidentiality. The Commission nevertheless were of the view that additional warrants should be obtainable for intrusions to prevent or detect additional charges pertaining to the individual earlier charged.

9.17 The Hong Kong Commission accordingly recommended that a ground for issuing a warrant authorising intrusions should be that it is for the purpose of preventing or detecting serious crime. They however noted that other jurisdictions impose additional requirements before a warrant should be issued, the two principal restrictions being that there is probable

cause for suspicion and the information is not reasonably acquirable by other means. The Commission referred to the United States Wiretap Act which requires that the authorising judge be satisfied that there is "probable cause for belief" that an individual has committed or is about to commit one of the specified serious offences. They noted that similarly, under the German law "exploratory" interceptions are not permitted and that in *Malone* the United Kingdom told the European Court that "likelihood of conviction" was applied as a requirement. The Commission stated that despite the White Paper's endorsement of this requirement, it was subsequently omitted from the Act and that Halsbury opines that it is nonetheless a precondition.

9.18 The Hong Kong Commission agreed that intrusions should only be lawful in relation to individuals reasonably suspected of offending and considered that the techniques should not be used for exploratory fishing expeditions, particularly so in view of the increased deployment of new technologies that facilitate telephone tapping with little effort, such as key word recognition. They noted that the United Kingdom Interception of Communications Act states that in determining whether a warrant is justified, a relevant matter is whether the information "could reasonably be acquired by other means" and that the United States Wiretap Act is more explicit in requiring that:

> "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."

9.19 The Hong Kong Commission further noted that the Canadian and German laws have similar provisions, the latter requiring that other investigatory methods would be ineffective or considerably more difficult. The Commission stated that they also endorsed this restriction that intrusions should not be authorised unless the information is not reasonably available by less intrusive means. They considered that these other, overt means will generally be more difficult so that the test must not only relate to the relative ease of deploying intrusive techniques, but the *reasonableness* of so doing. The Commission stated that this test would balance efficiency with the competing public interest in providing protection from surveillance, and in particular, they supported the rigorous provision of the United States law requiring the authorities to provide details of the difficulties which would arise from being restricted to conventional methods. The Commission accordingly recommended that a warrant should be issued for the prevention or detection of serious crime only where:

* there is probable cause for suspicion of the target; and
* the information is not reasonably available by less intrusive means.

9.20 The Hong Kong Commission was of the opinion that probable cause for suspicion is less apt for security than crime, and hence sections 3(2)(a) and 5(2)(a) of the United Kingdom Security Service Act 1989 and the Intelligence Services Act 1994 respectively provide that the intrusion must be thought:

> "necessary for the action to be taken in order to obtain information which ... is likely to be of substantial value in assisting the Service to discharge any of its functions; and cannot reasonably be obtained by other means"

9.21 The Hong Kong Commission therefore recommended a similar restriction on intrusions for the purposes of security, defence, or international relations in respect of Hong Kong, stating that intrusions should only be permitted where they are likely to be of substantial value in furthering security, defence, or international relations in respect of Hong Kong; and the information cannot be reasonably obtained by other means.

9.22 The Hong Kong Commission further pointed out that the United Kingdom Act also sanctions intrusions "for the purpose of safeguarding the economic well-being of the United Kingdom", noting that during the Second Reading the Home Secretary said of this expression:

> "As in the case of serious crime or national security the Secretary of State has to consider that interception is not just desirable. Secondly, interception has to be protective. It must be concerned with safeguarding the country's economic well-being, not with promoting it. That means it relates to threats to that well-being. Thirdly, it is the economic well-being of the United Kingdom which is at issue. By definition, the matter must be one of national significance and cannot be of a trivial kind which is peripheral to that well-being. It is a crucial part of our foreign policy to protect the country against adverse developments overseas, which do not necessarily affect our national security so directly as to justify interception on that ground but which may have grave and damaging consequences for our economic well-being, such as a threat to the supply of a commodity on which our economy is particularly dependent."

9.23 The Hong Kong Commission noted comments stating that this wording is "broad enough to catch the actions of multinational companies, currency speculators, and the diplomatic communications of Britain's EC partners." They remarked that it may be that this accords with current conditions pointing out that it is argued that with the end of the cold war secret services are increasingly concentrating on industrial espionage conducted by means of the usual

clandestine techniques, business executives and trade negotiators are bugged and tracked at home and abroad, and corporate telecommunications are regularly monitored and eavesdropped. The Hong Kong Commission considered that notwithstanding the prevalence of such state sponsored industrial espionage, a broad provision along United Kingdom lines would be inappropriate for Hong Kong. They believed, however, that the importance of protecting the Hong Kong currency peg to the US dollar merits special consideration. The Commission therefore recommended that one of the grounds for issuing a warrant should be that it is for the purpose of safeguarding the stability of the local financial system remarking that this should extend to intrusions conducted both within and outside Hong Kong.

9.24 The Interception of Communications Ordinance however contains the following provision setting out the following requirements for the issue of warrants:

> 4(2) An order shall not be made under this section unless it is necessary-
> (a) for the purpose of preventing or detecting a serious crime; or
> (b) in the interest of the security of Hong Kong.
> (3) In deciding whether it is necessary to make an order, the judge shall determine that-
>
> (a) there are reasonable grounds to believe that an offence is being committed, has been committed or is about to be committed;
> (b) there are reasonable grounds to believe that information concerning the offence referred to in paragraph (a) will be obtained through the interception sought;
> (c) all other methods of investigation have been tried and have failed, or are unlikely to succeed; and
> (d) there is good reason to believe that the interception sought will result in a conviction.

F. Duration of warrants

9.25 The Hong Kong Commission pointed out that section 4 of the United Kingdom Interception of Communications Act provides that warrants shall be issued for an initial period of two months and thereafter require renewal, also for a period of two months (but with provision for six months). They remarked that renewal requires that the Minister considers that the warrant "continues to be necessary" for the relevant purpose under section 2 and that the United Kingdom's two secret service Acts prescribe six months. The Commission further pointed out that six months is similarly the period prescribed under the Australian Act for both security (section 9(5)) and customs (section 21(5)), the Canadian Act adopts 60 days and that the United States Act is the most stringent as section 2518(5) stipulates 30 days.

9.26 The Hong Kong Commission thought that 60 days should suffice for both crime and security and that a similar period should govern extensions. They pointed out that they have considered but rejected adoption of an upper limit to the number of extensions given. The Commission considered that one possibility was that repeated extensions should be dealt with by a higher court, but thought on the other hand, that the initial determination of whether to approve a warrant is likely to be the most important determination. They therefore recommended that a warrant should be issued for an initial period of 60 days and that renewals may be granted for such further periods of the same duration where it is shown (according to the same criteria applied to the initial application) to continue to be necessary.

9.27 The Interception of Communications Ordinance sets out the duration and the requirements for renewal as follows:

> 6(4) Any authorization under a court order (4) Any authorization under a court order to intercept a communication shall be valid only for as long as it is necessary to achieve the purpose of the interception or, in any event, for a period not exceeding 90 days, after which, the said interception shall be deemed unlawful in accordance with section 3 unless its renewal is authorized under subsection (6).
> (5) An application for renewal of a court order by the authorized officer shall be made ex parte and in writing to a judge of the High Court in Chambers and shall be accompanied by a sworn affidavit stating-
> (a) the reason and period for which the renewal is required;
> (b) details of the times, dates and the type of interception conducted under the court order, and of such information obtained from the said interceptions; and
> (c) particulars of any previous applications involving the same person.
> (6) The judge may renew a court order only once for a period not exceeding 90 days, after which time, any continued interception shall be deemed unlawful under section 3.

G. Safeguards regarding retention of surveillance materials

9.28 The Hong Kong Commission noted that section 6 of the United Kingdom Act requires that the Secretary of State must make such arrangements as are necessary to ensure that-

- the extent to which the material is disclosed,
- the number of persons to whom any of the material is disclosed,
- the extent to which the material is copied,
- the number of copies made of any of the material,

is "limited to the minimum that is necessary" for the purposes under section 2 (i.e. the prevention and detection of serious crime etc.). They remarked that the *Preston* case made it clear that this provision restricting the currency of intercepted material was only workable where the purpose of the interception and the retention of the resultant surveillance materials was restricted to the "preventing and detecting" of crime:

> "With the handful of people in the public service engaged in the use of intercepts for the forestalling and detection of crimes this makes sense, but if the purpose includes the prosecution of offenders it is impossible to imagine that any 'arrangements' made by the Secretary of State under section 6 which would prevent the materials from being liberated into the trial process, as happened in *R v Effik*, after which any attempt to control their wider dispersion would be hopeless, thus compromising both the secrecy of the interception process and the privacy of those whose messages had been overheard."

9.29 The Hong Kong Commission stated that it became apparent during the trial in *Preston* (although no evidence was led to that effect) that the defendants' telephones had been tapped and the defendants sought access to material so derived to establish a defence (coercion). They noted that the Court held that section 6 required that intercept materials must be destroyed once police inquiries resulted in charges being laid, and it was this, rather than section 9's restrictions on admissibility which precluded the defendants from having the material admitted. The Commission further pointed out that under the United Kingdom scheme, the "shelf life" of surveillance materials is strictly limited, the timing and specific purposes of intrusions must be specified in the warrant and upon fulfilment of those purposes the material obtained pursuant to the warrant must be immediately destroyed and hence may not be used as evidence. They stated that the destruction of the material protects the privacy of targets and their contacts and controls providing some accountability are provided at another level. The Hong Kong Commission were of the view that the appeal of this approach is that it disposes of some basic difficulties which would otherwise arise from retention of the material and such a system arguably sustains public confidence.

9.30 The Hong Kong Commission consequently recommended the adoption of provisions similar to section 6 of the United Kingdom Interception of Communications Act 1985, including the imposition of a requirement on the warrant-issuing authority to ensure that adequate steps are taken to achieve compliance with the stipulations set out above. They stated that their adoption of provisions along the lines of section 6 will have the result that evidence of the fruits of *authorised* surveillance will never be available in a prosecution: their purpose has been spent

in addressing the earlier stage of the fight against crime, namely prevention and detection, and must thereupon be destroyed. They further stated that as regards unauthorised surveillance, such materials would necessarily escape the statutorily imposed requirements regarding its destruction, and such materials would accordingly be available as evidence in a subsequent prosecution. (The provision seeking to provide for this matter in the Interception of Communications Ordinance is noted in par 9.44 below.)

H. Admissibility of surveillance materials

9.31 The Hong Kong Commission noted that under general common law principles, the admissibility of evidence is solely determined by the relevance of the evidence and that there is, however, a judicial *discretion* to exclude unfairly obtained evidence. They remarked that United States law prohibits the admission of illegally obtained evidence and supporters of this approach argue that this both discourages illegal methods and concentrates the minds of investigators on more straight-forward means of investigation. The Commission however pointed out that deeming illegally obtained surveillance materials inadmissible would not preclude investigators from using it during the investigation, such as confronting suspects with the materials to elicit confessions.

9.32 The Hong Kong Commission noted that under the United Kingdom Act, these questions do not arise as regards telephone tapping because section 9 prohibits any reference to this intrusion, whether it is authorised or unauthorised. They remarked that it provides that in any proceedings of a court or tribunal "no evidence shall be adduced and no question in cross examination shall be asked which tends to suggest" that an intercept has or will occur, whether authorised by warrant or not. They noted that it will be recalled that the genesis of this legislation was just such a question! The Commission pointed out that the court in *Preston* concluded that the "otherwise impenetrable" section 9 only made sense on the basis of a narrower interpretation of section 2:

> "If the purpose of Parliament was to allow the intercept materials to become part of the prosecution process it is hard to see any point in a provision which would make it ... impossible to use them in that process ... . By contrast, on the narrower reading of s. 2 there would be no need to make explicit provision for the admissibility of materials which by virtue of s. 6 would no longer exist, and the purpose of s. 9 can be seen as the protection, not of the fruits of the intercepts, but of the information as to the manner in which they were authorised and carried out."

9.33 The Hong Kong Commission noted that in Hong Kong there was at that stage no bar to the defence raising the issue of tapping, provided it is relevant to the case and that usually, this would not be relevant, because it would relate to that part of the investigation which would be adequately referred to in the trial that as a result of "information received" the police were at the scene of the attempted crime. They remarked, however, that given the breadth of their proposed offences criminalising surveillance and the interception of communications, adoption of a provision along the lines of section 9 would have the effect of generally prohibiting the admissibility of evidence of all surveillance and interception activities. The Commission pointed out that this is not the United Kingdom position, because there only the interception of communications is prohibited, and that even this prohibition has been narrowly defined. They remarked that it will be recalled that in *R v Effik* an interception was effected without a warrant and that the court concluded that no warrant was required because the interception was not prohibited, as it had been conducted outside a public telecommunications system. The Commission pointed out that section 9's restrictions were not applicable as such, and the evidence, not being excluded by statute, was admissible. The Hong Kong Commission considered, however, that their much broader prohibitions on surveillance and interception of communications should catch intrusions across the board and a provision in similar terms to section 9 would render any reference to such activities inadmissible, whether or not it was authorised.

9.34 The Hong Kong Commission remarked that they were initially disposed to agree that surveillance materials pertaining to the period preceding the laying of the charge should be able to be used in the subsequent prosecution, on the basis that it would help address the serious international crime problem facing Hong Kong. They noted that while evidence arising from intercepts is not usually admitted in Hong Kong, in a then recent major drug case it was. They pointed, however, out that in that case, the calls were intercepted by the Royal Canadian Mounted Police. They also noted that the United States, Canada, and Australia all countenance the admission of surveillance materials as evidence in prosecutions.

9.35 The Hong Kong Commission recognised, however, that the use of surveillance/intercept materials as evidence will require their retention for this purpose, and furthermore, that not only does this pose the risk of dissemination, but the inevitable outcome of their use as evidence. They pointed out what is more, it is *public* dissemination which will result, and in other words,

use as evidence will necessarily seriously compound the invasion of privacy entailed by the original intrusion. The Commission considered that in addition to this objection in principle, there are practical difficulties about retaining surveillance materials for use as evidence. They considered that only a small part of such materials would be used by the prosecution and the remainder of the police evidence would have to be provided to the defence as unused material, and it would be a matter for the court to impose appropriate conditions. The Hong Kong Commission remarked that for example, defence counsel may have to undertake not to divulge the contents of tapes played to them. They were of the view that the legal status of unused materials was vexed and noted that it was subject to a number of appeals. The Commission noted that a further complication which is avoided by prohibiting the use of surveillance materials as evidence arises from the application of public interest immunity. The Hong Kong Commission therefore recommended that for these reasons, materials obtained through surveillance or interception should be inadmissible as evidence, regardless of their relevance. They also rejected any qualification of their endorsement of the United Kingdom Act's provisions whereby such materials will be destroyed once an investigation moves into prosecution mode. The Commission furthermore recommended the adoption of the United Kingdom's prohibition on the admission of evidence obtained by means of unauthorised surveillance or interception of communications, remarking that the prohibition should cover not only the fruits of surveillance but also details of methods used.

9.36 The Hong Kong Commission noted that this approach apparently accords with existing Hong Kong practice and that according to a press report the approach adopted in *Preston* accords with current practice in Hong Kong. They pointed out that it was reported in February 1992 that Acting Deputy Secretary of Security, Mr Clinton Leeks, told the Omelco Constitutional Development Panel that all interceptions were in connection with investigations and were not part of evidence-gathering for court cases. The Commission thought that a major advantage of adopting the United Kingdom requirement that surveillance and intercept materials be destroyed and hence unavailable as evidence is that this provides a significant disincentive to undertaking surveillance in the first place. (The provision seeking to provide for this matter in the Interception of Communications Ordinance is noted in par 9.44 below.)

l. Notification following termination of surveillance

9.37 The Hong Kong Commission noted that several other jurisdictions impose a requirement

that upon the termination of surveillance, the target should be informed of that fact. They considered that in principle, such a notification requirement should increase the accountability of those engaging in intrusions. They remarked that a requirement that the subject of surveillance be notified of that fact once the surveillance has been discontinued is a feature of some but not all laws. The Hong Kong Commission pointed out that section 2518 of the United States Wiretap Act prescribes detailed procedures and that it is also a feature of the German law. They noted that one aspect of the German law which was challenged in *Klass* is that there was no requirement that the subject of surveillance be *invariably* notified upon its cessation. The Commission pointed out that the European Court held that this was not inherently incompatible with the privacy provision of the European Convention, provided that the person affected be informed as soon as this could be done without jeopardising the purposes of the surveillance. The Hong Kong Commission considered that this indicates that a post-surveillance notification requirement is desirable in terms of compliance with the Bill of Rights. They remarked that the basis of a notification requirement is two-fold, namely firstly it marks the seriousness of the earlier intrusion into privacy, and the requirement would introduce an important element of accountability which should deter the authorities from tapping unnecessarily, and secondly the individual should be able to challenge the grounds on which the intrusion had been granted. The Commission considered that denying the subject of surveillance such information will tend to undermine the efficacy of these mechanisms enhancing accountability, such as complaints procedures and the provision of compensation awarded for wrongdoing. They noted that the United Kingdom Act lacks a notification requirement and, although compensation is provided for, no claim to the date of the Consultation Paper has been successful.

9.38 The Hong Kong Commission thought that the public has a right to be told the extent to which intrusions were occurring, although this would also be addressed by public reporting requirements. They considered that the adoption of a notification requirement along the above lines would diminish the need for mechanisms at the stage when the warrant was approved, such as the participation of a friend of the court. They however recognised that merely to inform an individual of the fact that he had been the subject of surveillance would be unhelpful. They were of the view that more helpful and informative would be to notify the former target of the sorts of matters covered by the United States provision, including, where appropriate, providing the intercept materials themselves. The Commission explained that they understood that under the then current Hong Kong interception arrangements often only key points would

be abstracted and retained. They considered in regard to the destruction of the intercept materials prior to notification would largely destroy the basis of the notification mechanism, but also recognised that "destruction" is not an absolute concept in the digital age.

9.39 The Hong Kong Commission were furthermore of the view that a notification requirement would have to be made subject to a proviso ensuring that the operational effectiveness of investigative agencies would not be diminished. They considered that the requirement would have to be couched in terms that, following the cessation of surveillance, the subjects should be notified unless this would "prejudice" the purposes of the original intrusion. The Commission noted further that there would also need to be provision for postponement of the notification on the same grounds. They also referred to the *Preston* case which indicates that the traditional United Kingdom approach of surveillance is that it is necessarily clandestine and that merely divulging that it has occurred would be prejudicial:

> "Those who perform the interceptions wish to minimise the dissemination of the fact that they have been performed, since it is believed that this would diminish the value of activities which are by their nature clandestine. We need not consider to what extent this preoccupation with secrecy at all costs is soundly based for it has been treated as axiomatic for decades, if not longer."

9.40 The Hong Kong Commission noted that this is one approach and may be referred to as the "clandestine imperative" - i.e. that people should be generally kept in the dark about the incidence of surveillance. They remarked that the difficulty is that applying the "prejudice" test on this basis would effectively negate the requirement of notification. The Commission was of the view that that requirement would be illusory, since notification would necessarily conflict with the clandestine imperative and would therefore never occur. They considered that if there is to be a requirement, it must be clarified and tightened up before its full implications can be assessed. The Commission further pointed out that there is the additional aspect of the content of the notification to the ex-target - should this be restricted to the mere fact of notification or extend to other matters, including surveillance materials. This would also need to be determined by the application of an explicit prejudice test.

9.41 The Hong Kong Commission considered that for the requirement to be meaningful, it would have focus to on actual prejudice in the particular circumstances of the case and that such a test depends on whether the surveillance is in respect of the target or an innocent party:

* Prejudicial in relation to the particular target could be defined to cover the situation where the target is likely to be the subject of surveillance in the future and notification is likely to make such surveillance more difficult. This approach would preclude notification of recidivist offenders, or those where there was a reasonable prospect that the investigation may be reopened in the future.
* The most obvious grounds on which it would be prejudicial to notify innocent parties in particular cases is if they could be expected to alert the target. Another possibility is that the authorities may wish to tap the innocent party in order to further tap the target again and alerting the innocent contact may make this more difficult.

9.42 The Hong Kong Commission noted the following implications of applying a more rigorous notification requirement:

* The provision of the fruits of surveillance/intercept following its cessation assumes that they are still in existence, and a robustly applied notification requirement would necessitate their retention when all other purposes had been fulfilled. The difficulty with this is that the retention of surveillance materials has its own privacy risks.
* Should the notification requirement be applied meaningfully, it will require the relevant authority to make an informed decision as to whether notification should be effected, applying criteria along the above lines. Consideration would need to be given to the extent of the information given to the ex-target under a notification requirement. This raises potentially complex issues and would require the relevant authority to be well briefed on a case by case basis, applying the prejudice test outlined above, and the massive resource implications are obvious.

9.43 The Commission stated that there is also the question as to who should determine whether the subjects should be notified, and the contents of such notification. In the United States this is done by a judge. They remarked that they have proceeded, up to that point, on the basis that decisions impinging on surveillance/interceptions should be capable of review, however, if decisions regarding notification were similarly to be reviewed the resource implications would be even greater. They considered that since they recommended that surveillance materials be inadmissible, there is less need for a notification requirement in Hong Kong than in those jurisdictions where surveillance materials may be produced at the trial. They noted that in the United States and Canada the apparent practice is only to notify the

public of the fact of surveillance and it is presumably due to this that those jurisdictions have not apparently encountered the difficulties the Hong Kong Commission envisaged may result from a more extensive notification requirement. They thought that such a restricted notification requirement is of little benefit and that identifying the range of innocent parties meriting such notification remains problematic. Finally, they believed that the accountability aspect is more directly addressed by the warrant requirement and accordingly rejected a notification requirement. In doing so, the Hong Kong Commission's main concerns were that such a scheme would have considerable resource implications, without a clear concomitant benefit.

9.44 The following provision was adopted in the Interception of Communications Ordinance in regard to notification following termination of surveillance and the admissibility of information obtained by an interception:

> 7(1) Where a court order has been terminated by the judge or has expired and has not been renewed, all intercepted material obtained under that court order shall be placed in a packet and sealed by the authorized officer, and that packet shall be kept away from public access.
> (2) Where a charge is laid against the person named in the court order, the authorized officer shall notify the judge who may order the release of the intercepted material to the prosecutor where the latter intends to tender the intercepted material as evidence in criminal proceedings.
> (3) Where the prosecutor intends to tender the intercepted material as evidence in criminal proceedings, he shall notify the accused of this intention at least 10 days before the trial date and furnish him with-
> (a) a copy of the application made under section 5;
> (b) a copy of the court order;
> (c) a copy of the application for renewal of the court order, if any.
> (4) Any information obtained by an interception that, but for the interception, would have been privileged remains privileged and inadmissible as evidence without the consent of the person enjoying the privilege.
> (5) Where no charge is laid against the person named in the court order within 90 days of the termination of a court order, the court shall inform the authorized officer of its intention to-
> (a) destroy the intercepted material in the sealed packet; and
> (b) notify the person named in the order that his communications have been intercepted,
> and shall give the authorized officer 5 days to inform the court whether or not he wishes to challenge the court's intentions.
> (6) Where the authorized officer wishes to challenge the court's intentions stated in subsection (5)(a) or (b), he shall in writing provide the judge with his reasons for opposing the court's said intentions and it shall remain within the judge's discretion whether or not to accept these reasons.
> (7) Where-
> (a) the authorized officer does not inform the court of his intention to challenge the

court's intentions stated in subsection (5)(a) or (b) within 5 days; or

(b) after considering the authorized officer's reasons for preventing the court from carrying out its intentions, the court decides not to accept his reasons,

the court shall order that all intercepted material in the sealed packet be destroyed immediately and shall notify the person named in the order that his communications have been intercepted, providing in the notice details on-

(i) the type of communication that was intercepted;

(ii) the time and date of each interception; and

(iii) the reasons for conducting the interception.

(8) Where the judge exercises his discretion not to order the destruction of intercepted material, he may make an order to specify the period for which the intercepted material will remain undestroyed.

J. The regulation of surveillance

9.46 The Hong Kong Commission noted that whereas the United Kingdom and Australia have a specially constituted administrative body tasked to monitor the application of the approvals system, in the United States the relevant authority simply collates and publishes the data received. They remarked that this parallels the respective countries' data protection regimes, with only the United States lacking a true supervisory authority. They stated that as between the United Kingdom and Australia, the latter's Ombudsman is full-time (as are his subordinates) but intercepts are only one of his office's concerns. The Hong Kong Commission also remarked that the United Kingdom Commissioner is part-time but in that capacity focuses solely on supervising intercepts whereas their recommendations, however, cover not only interceptions but also surveillance and this would generate more work.

9.47 The Hong Kong Commission considered that a monitoring body was necessary and that a requirement that the subject of surveillance be subsequently notified of that fact would reduce review issues in those cases. They pointed out that notification would equip the individual with explicit grounds to challenge the issue or application of the warrant, but that they have rejected a notification requirement and the issue of independent review therefore becomes crucial: as the individual will not be in a position to challenge the surveillance it is essential that another party scrutinise the matter on his behalf.

9.48 The Hong Kong Commission recommended that warrants should be issued by a High Court judge, unlike the procedure in the United Kingdom where warrants are authorised by a minister. They noted that such a decision would have to be made pursuant to an ex parte application and as ex parte applications are held in secret there is generally a right vested in

the excluded party to have the order subsequently discharged. They considered that the review of whether a warrant had been properly issued would necessarily also have to be decided by a judge, albeit one more senior. They were of the view that this supervisory function should be concentrated instead of dispersed to enable the authority to obtain an overview of the incidence of surveillance throughout society, such as whether any particular segments were being targeted. The Commission therefore recommended that a Justice of Appeal should be appointed as the supervisory authority to review the issue of warrants authorising surveillance or the interception of communications and that the applicable criteria should be those of judicial review.

9.49 The Hong Kong Commission explained that the main control they envisaged being undertaken by the supervisory authority would be checking that the reasons given in the affidavits supporting the issue of the warrant were genuine and that the warrant had been executed in accordance with its conditions. They noted that a warrant may not have been properly issued, either because the statutory requirements had not been properly applied, or because the supporting affidavits may be false - a not uncommon occurrence in Hong Kong with Anton Piller applications. They thought that it should be left to the supervisory authority to determine which warrants should be examined and on what basis. The Commission considered that there would in any event be judicial review proceedings open to individuals who became aware of the issue of the warrant, as well as proceedings for damages. They also recommended that the supervisory authority should be empowered to review cases at the request of an aggrieved individual. The Hong Kong Commission pointed out that apart from the question of whether the warrant has been properly issued, the other area for supervision relates to whether the warrant had been complied with and recommended that this area should also be dealt with by the supervisory authority.

9.50 The Hong Kong Commission remarked that the United Kingdom Commissioner for interceptions is solely concerned with whether *authorised* taps have complied with statutory requirements, and, furthermore, the Commissioner accepts that if interception without authorisation under a warrant were taking place, there would be no reason for such conduct to come to his attention. The Commission also pointed out that the Australian Commonwealth Ombudsman is not subject to this restriction, would be entitled to investigate unauthorised taps but that he is nonetheless, not specifically tasked to endeavour to detect such taps, nor would he be equipped to do so.

9.51 The Hong Kong Commission stated that they were initially disposed to endorse the need for the supervisory authority to pursue allegations of improperly issued warrants, or intrusions not sanctioned by a warrant. They considered, however, that to initiate such an inquiry, the supervisory authority would need grounds for believing that there had been a contravention of the statutory requirements. Furthermore, as it is impossible to eliminate the possibility of technical surveillance, mere suspicion would not suffice, nor would the authority be itself equipped to investigate whether unauthorised intrusions were occurring. They considered that such unauthorised intrusions would in any event be a criminal matter for investigation by the relevant law enforcement agency. The Hong Kong Commission stated that the supervisory authority would in practice then be restricted to checking the paperwork provided by the relevant agency, and if that were the case, the only issue would be whether a warrant had been issued and, if so, whether it had been issued on proper grounds. They remarked that improper issue would usually be attributable to false supporting affidavits. The Commission noted that the effective exclusion of the investigation of unauthorised warrants coincides with the United Kingdom position, which becomes explicable on this basis. They therefore concluded that the supervisory authority should be restricted to investigating whether a warrant had been properly issued.

K. Reports

9.52 The Hong Kong Commission noted that the three jurisdictions considered by them endorse a degree of transparency about interception activities and that this is achieved by publishing statistics on the number of authorised taps. They pointed out that the only data provided by the United Kingdom Commissioner's annual report is the number of authorised taps and that the Commissioner has repeatedly said that the number of warrants is a misleading guide to the number of lines tapped, but has declined to indicate the number of people affected. The Hong Kong Commission remarked that the figures on taps are widely thought to understate the position (e.g. the Act allows one warrant to authorise the interception of communications to or from any number of addresses) and the lack of detail on other matters lends scope for manipulation of the figures. The Commission remarks that by way of contrast, the United States reports give a very detailed (and graphic) picture and as a result, United States citizens and administrators are given a full picture of the incidence, cost, and

effectiveness of intercepts engaged in for law enforcement purposes.[22] The Hong Kong Commission remarks that those engaged in such intrusions are accordingly accountable.

9.53 The Hong Kong Commission drew attention to the fact that they argued that the main benefit of a notification requirement is that it increases accountability and that they rejected such a requirement for practical reasons. They remarked that detailed annual reports provide, however, an alternative method of achieving accountability and that they believed that reports play a crucial role in increasing public accountability for surveillance. Hence, they recommended that the supervisory authority should furnish annually a confidential report to the Governor and a public report to the Legislative Council. They also pointed out that unlike section 8(8) of the United Kingdom Act, they preferred, however, to specify the different matters which must be included in the reports. They further stated that the United States report focuses on the cost effectiveness of interceptions, but in their view this cannot be assessed in purely financial terms. The Hong Kong Commission pointed out that intercepts were becoming increasingly cheap and considered that the more relevant cost is that of the intrusion into the individual's privacy. They were of the view that the privacy costs to the community would be indicated by figures on the number of persons intercepted and the number of communications intercepted. They therefore recommended that there should also be a statutory requirement that the following matters be covered:

* the number of warrants authorised;
* their average length and their extensions;
* the classes of location of the surveillance, i.e. domestic, business etc.;
* the type of surveillance device used; and
* the number of persons arrested and convicted as a result of the surveillance or intercepts.[23]

9.54 The Hong Kong Commission remarked that the confidential annual report to the

---

22 These reports are even available on the Internet, see http://www.uscourts.gov/wiretap/contents.html for the *1997 Wiretap Report.*

23 The Hong Kong Commission considered this item important because it would indicate the yield of the intrusions and would make the authorities accountable to the community regarding their utility. They considered if large scale surveillance was resulting in few arrests or convictions the community would be entitled to question whether the privacy costs were justified by the results.

Governor would cover such matters as were required by the Governor, or considered relevant by the supervisory authority, such as for instance, information on particular segments of the population being targeted might be considered relevant. The Commission noted that in the *Preston* case it was pointed out that:

> "Those who perform the interceptions wish to minimise the dissemination of the fact that they have been performed, since it is believed that this would diminish the value of activities which are by their nature clandestine."
>
> "... the purpose of s. 9 [is] the protection, not of the fruits of the intercepts, but of information as to the manner in which they were authorised and carried out. ... the defendant was not to have the opportunity to muddy the waters at a trial by cross-examination designed to elicit the Secretary of State's sources of knowledge or the surveillance authorities' confidential methods of work."

9.55 The Commission remarked that even accepting the rationale of this approach, they did not think that publication of informative reports along these lines will "diminish the value" of surveillance activities. They considered that because the figures would be couched in anonymity regarding the persons targeted it cannot be argued that their publication could prejudice the purposes of the original intrusion in particular cases. They said they would question the claim that the dissemination of even general data could have adverse consequences, but in any event considered that considerations of accountability should prevail. The Hong Kong Commission stated that they believed that people should know the extent of surveillance in their society.

9.56 The following provision was, however, included in the Interception of Communications Ordinance:

> 11. The Legislative Council may at any time require the Secretary for Security to provide, for any specific period, the following information, namely-
> (a) the number of interceptions authorized and denied;
> (b) the nature and location of the facilities from which and the place where the communications have been interpreted;
> (c) the major offences for which interception has been used as an investigatory method;
> (d) the types of interception methods used;
> (e) the number of persons arrested and convicted as a result of interceptions;
> (f) the average duration of each interception; and
> (g) the number of renewals sought and denied.

L. Remedies

9.57 The Hong Kong Commission stated that in their view, the United Kingdom's provisions for monetary compensation are illusory since they are restricted to breaches of statutory requirements in the issue of warrants and unauthorised taps are not compensable. They note that no compensation has, not surprisingly, been awarded to date by the specially constituted tribunal, and that, on the other hand, both the United States and Australian laws provide aggrieved parties with a statutory right to claim in court monetary recompense for unauthorised intercepts. They pointed out that they doubted the feasibility of investigating whether unauthorised surveillance has been conducted. They nonetheless considered, whilst it would be unusual for an individual to learn that he had been subject to unauthorised surveillance, this would happen from time to time. Hence, they recommended that compensation should be payable for unauthorised intrusions, explaining that providing for compensation provides an additional sanction and provides both a norm and a deterrent.

9.58 The following provision was adopted in Hong Kong:

> "10(1) This part applies to an interception an interception of a communication in the course of its transmission by post or by means of telecommunication system through the use of any electro-magnetic, acoustic, mechanical or other device in contravention of section 3.
> (2) For the purposes of this Part, a person is an aggrieved person if and only if-
> (a) the person was a party to the communication; or
> (b) the communication was made on the person's behalf.
> (3) If a person ("the defendant")-
> (a) intercepted a communication in contravention of section 3; or
> (b) disclosed intercepted material to another person in contravention of section 9(1) or (5),
> a court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the interception or the disclosure of intercepted material by making such orders against the defendant as the court considers appropriate.
> (4) If a court convicts a person ("the defendant") of-
> (a) an offence under section 3; or
> (b) an offence under section 9(1) or (5),
> the court may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the interception or the disclosure of the intercepted material by making such orders against the defendant as the court considers appropriate.
> (5) Without limiting the orders that may be made under this section against a person ("the defendant"), a court may make an order of one or more of the following kinds-
> (a) an order declaring the interception or the disclosure of intercepted material, as the case requires, to have been unlawful;
> (b) an order that the defendant pay to the aggrieved person such damages,

including punitive damages, as the court considers appropriate; or

(c) an order in the nature of an injunction.

(6) Without limiting the orders that may be made by a court under this section, an order may-

(f) include such provisions as the court considers necessary for the purposes of the order; and

(g) be made either unconditionally or subject to such terms and conditions as the court determines.

(7) A court may revoke or vary an order in the nature of an injunction made by the court under this section.

(8) An application under subsection (3) for the grant of remedial relief is to be made within 6 years from the date on which the aggrieved person discovered the interception, or the disclosure of the intercepted material, as the case may be.

(9) An application under subsection (4) for the grant of remedial relief is not subject to any limitation period, but must be made as soon as practicable after the conviction concerned."

M. Supervisory tribunal

9.59 The Hong Kong Commission noted that in addition to establishing a supervisory authority, section 7 of the United Kingdom Act establishes an independent tribunal to investigate complaints regarding the issue of warrants. Hence, a person who believes himself the subject of interception may apply to the Tribunal for an investigation of whether a warrant has been issued and if so whether this has been done in accordance with the Act. They pointed out that this jurisdiction does not extend to unauthorised interceptions: under section 1 that is a criminal offence and its investigation is therefore a police matter. The Hong Kong Commission remarked that their reasons for concluding that it is not feasible for the supervisory authority to investigate unauthorised surveillance apply equally to a complaints tribunal. They furthermore recommended that the supervisory authority be empowered to pursue complaints. Finally, they recommended that aggrieved individuals be able to pursue claims for compensation in the courts. The Hong Kong Commission therefore remarked that for these reasons, they we do not consider that a separate complaints tribunal will be required to supplement the role of the supervisory authority.

N. Licensing of surveillance equipment

9.60 The Hong Kong Commission noted that section 8 of their Telecommunication Ordinance imposes restrictions on the possession or use of surveillance devices. They remarked that a wide variety of scanners and receivers are available in Hong Kong, which are apparently sold

on the understanding that the buyers are tourists and the equipment will be exported. They pointed out that some 50 shops are reported to be selling surveillance equipment in Tsim Sha Tsui and Central alone. The Hong Kong Commission was of the view in view of this apparent lack of effectiveness of existing controls on the availability of surveillance equipment, that they were unable to recommend the enactment of any additional legislative controls on this matter. An additional reason stated by them is that their proposals target surveillance whenever it is conducted by a "sense-enhancing, transmitting or recording device" and that this would encompass not only the comparatively specialised apparatus regulated by the Telecommunication Ordinance but also ordinary items such as tape recorders and binoculars. They therefore considered that it is plainly unrealistic to endeavour to impose a licensing regime in respect of such items.

CHAPTER 10

THE LEGAL POSITION IN CANADA

A. Introduction

10.1 In the case of *Michaud v Quebec (Attorney General)* Chief Justice Lamer of the Supreme Court of Canada summarised the Canadian position on interception of private communications as follows:[1]

> 20. The *Protection of Privacy Act*, S.C. 1973-74, ... was adopted to fill a troubling statutory void by establishing a comprehensive regime for the regulation of electronic surveillance. Prior to the Act, law enforcement officials were subject to few legal restrictions on their ability to intercept private communications, and the historical record suggests that this intrusive state power was frequently exercised well prior to Parliament's intervention. ... The core purpose of the Act was to enact a general regime for regulation of such surveillance in an effort to balance society's interest in the detection of crime, particularly organized crime, with an individual's right to personal privacy. The central means by which the Act effected its purpose was to impose a general ban on the interception of private communications in the absence of prior authorization. As this Court described the careful legislative balance of the Act in *R. v. Duarte*, [1990] 1 S.C.R. 30, at pp. 44-45:
>
> > Electronic surveillance plays an indispensable role in the detection of sophisticated criminal enterprises. Its utility in the investigation of drug related crimes, for example, has been proven time and again. But, for the reasons I have touched on, it is unacceptable in a free society that the agencies of the state be free to use this technology at their sole discretion. The threat this would pose to privacy is wholly unacceptable.
> >
> > It thus becomes necessary to strike a reasonable balance between the right of individuals to be left alone and the right of the state to intrude on privacy in the furtherance of its responsibilities for law enforcement. Parliament has attempted to do this by enacting Part IV.1 of the *Code*. An examination of Part IV.1 reveals that Parliament has sought to reconcile these competing interests by providing that the police must always seek prior judicial authorization before using electronic surveillance. [Emphasis added.]
>
> 21. To enforce this ban, the Act armed the individual surveillance target with the means to retroactively challenge the legality of a wiretap following the termination of the surveillance. More specifically, s. 4 of the Act created a civil action in damages against the Crown in right of Canada for unlawful interception of private communications: ... This right of action has since been complemented by provincial laws which create a delictual right of action against provincial authorities and others who engage in the interception of private communications without lawful authorization. ...
>
> 22. The Act, in large part, was modelled on comparable legislation adopted by the U.S. Congress under Title III of the *Omnibus Crime Control and Safe Streets Act of 1968*, June 19, 1968, Pub. L. No. 90-351, Title III, § 802, now codified as 18 U.S.C. §§ 2510-20 (1994) (hereinafter "Title III"). In light of the "striking similarities" between the two statutes, commentators

---

1 *Michaud v Quebec (Attorney General)* [1996] 3 SCR accessed at http://www.droit.umontreal.ca/doc/csc-scc/cgi-bin/repere.cgi?corpus=pub_en&tout=interception+private communications on 19/11/1998.

have concluded that the U.S. jurisprudence on Title III provides an "invaluable" source of guidance for issues arising under the Act. ... This Court has relied on Title III as a helpful tool for interpreting the scope of Part VI in light of the "remarkable similarity" between the two legislative regimes: *Lyons v. The Queen*, [1984] 2 S.C.R. 631, at p. 680, *per* Estey J. However, this Court has drawn inferences from important differences between the two regimes: *R. v. Thompson*, [1990] 2 S.C.R. 1111, at p. 1137 (specific minimization requirement under Title III); *Dersch*, *supra*, at p. 1511 (specific requirement of delivery of application to accused prior to trial under Title III).

23. Under Part VI of the *Criminal Code*, law enforcement officials may apply for an authorization to execute an electronic surveillance upon an *ex parte* application filed with supporting affidavits to a designated judge. Under s. 186(1), a judge may authorize an interception of private communications if the judge is satisfied that "it would be in the best interests of the administration of justice to do so". This Court explained in *Duarte*, *supra*, at p. 45, that the "best interest of the administration of justice" requires, at a minimum, that law enforcement officials have demonstrated reasonable and probable grounds that an offence has been committed and that communications relating to the offence will be intercepted. If the court issues an authorization, the surveillance must be carried out in accordance with the terms and conditions of the authorization. Within 90 days following the expiration of the authorization, the Crown must then deliver a written notification to the surveillance target stating that an authorization had been issued and executed, but the notice is not required to disclose the contents and details of the authorization. See s. 196(1).

24. Following completion of the *ex parte* hearing for authorization, the *Code* dictates that the application and supporting affidavits are "confidential" and shall be "placed in a packet and sealed" by a designated judge. However, Parliament created a statutory mechanism for seeking a judicial order to open and examine the packet under s. 187(1)(*a*)(ii) (originally R.S.C. 1970, c. C-34, s. 178(1)(*a*)(ii)). ...

The provision permits a broad range of unspecified parties to apply for an order under s. 187(1)(*a*)(*ii*). However, it provides no guidance as to what conditions would warrant a disclosure order. The virtually unanimous view is that Parliament originally intended to leave such issues to the discretion of the court rather than to create an automatic right to access to the packet to specific parties in specific circumstances. See *Dersch*, *supra*, at p. 1510, *per* Sopinka J. ("Parliament, therefore, intended to confer on the judge an unlimited discretion"); *R. v. Garofoli*, [1990] 2 S.C.R. 1421, at p. 1479, *per* McLachlin J. ("[T]he matter is in the discretion of the judge hearing the application"); *R. v. Durette*, [1994] 1 S.C.R. 469, at p. 491, *per* Sopinka J. ("The judge hearing an application under this section has a broad discretion to decide whether or not to provide access"), and at p. 518, *per* L'Heureux-Dubé J. ("[The legislator] left the courts with the task of deciding the proper approach to the matter"). Nonetheless, the state's interest in the confidentiality of its investigations was intended to be a major consideration in the judicial exercise of this discretion. As Sopinka J. described this state interest in *Dersch*, *supra*, at p. 1510:

> The purpose of the confidentiality provision of this section is apparently to ensure that the investigation is kept secret during the currency of the authorization and to protect informers, police techniques and procedures once the authorization is spent.
>
> And as McLachlin J. expressed in her dissent in *Garofoli*, *supra*, at p. 1480:
>
> "Parliament's dominant intention was that the documents [within the packet] should remain confidential".

25. This particular statutory provision has since been amended by Parliament in response to this Court's rulings in *Dersch* and *Garofoli*. In 1993, Parliament recast Part VI to give legislative recognition to the accused's constitutional right to examine the packet prior to trial. ...

Under this new legislation, it is clear that both an accused person and a non-accused person are entitled to apply for access to the packet. However, consistent with *Dersch*, Parliament adopted a mandatory regime of disclosure for an accused person. Under the new legislation, an accused is entitled to apply for access to the packet to prepare for trial under either s. 187(1.3) or 187(1.4); following appropriate blacklining by the Crown under the procedure stipulated by s. 187(4), the Crown "shall" deliver the edited wiretap application and affidavits to the accused in accordance with s. 187(5). But in contrast to this mandatory regime, Parliament specifically chose to preserve a discretionary regime of disclosure in addressing applications by non-accused

persons. A non-accused person may apply for access to the packet under s. 187(1.3), but Parliament specifically omitted to stipulate that the Crown "shall" deliver the contents of the packet in response to such a request.

26. The drafting of both s. 187(1)(*a*)(ii) and the recent s. 187(1.3) closely parallels the applicable U.S. legislation. Under the scheme of Title III, a wiretap application is similarly sealed following approval of the authorization. However, an individual who faces criminal prosecution on the basis of intercepted communications is entitled to examine the confidential application prior to trial; as noted in *Dersch*, at p. 1511, unlike Part VI of the *Code*, § 2518(9) of Title III specifically provides that copies of the wiretap application must be delivered to an accused 10 days before trial in order to extend the accused adequate opportunity to seek suppression of the wiretap evidence. On the other hand, where a non-accused individual seeks to examine the application, § 2518(8)(d) stipulates that a court enjoys a discretion to withhold access in the absence of a showing of "good cause".

...

In short, both s. 187(1)(a)(*iii*) and § 2518(8)9d) leave it to the court's discretion to balance the state's interest in the confidentiality of the packet against the individual's interest in privacy.

10.2 In the earlier case of *R v Duarte*[2] the Canadian Court the court noted that a reasonable balance between the right of individuals to be left alone and the right of the State to intrude on privacy in the furtherance of its responsibilities for law enforcement should be struck:

> The rationale for regulating the power of the state to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it (see definition section of Part IV.1 of the Code) has nothing to do with protecting individuals from the threat that their interlocutors will divulge communications that are meant to be private. No set of laws could immunize us from that risk. Rather, the regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.
>
> The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States v White*, supra, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.
>
> This is not to deny that it is of vital importance that law enforcement agencies be able to employ electronic surveillance in their investigation of crime. Electronic surveillance plays an indispensable role in the detection of sophisticated criminal enterprises. Its utility in the investigation of drug related crimes, for example, has been proven time and again. But, for the reasons I have touched on, it is unacceptable in a free society that the agencies of the state be free to use this technology at their sole discretion. The threat this would pose to privacy is wholly

---

2 See http://www.droit.umontreal.ca/doc/csc-scc/cgi-bin/repere.cgi?corpus=pub_en&toutR+v+Duarte accessed on 22/11/1998.

unacceptable.

It thus becomes necessary to strike a reasonable balance between the right of individuals to be left alone and the right of the state to intrude on privacy in the furtherance of its responsibilities for law enforcement. Parliament has attempted to do this by enacting Part IV.1 of the Code. An examination of Part IV.1 reveals that Parliament has sought to reconcile these competing interests by providing that the police must always seek prior judicial authorization before using electronic surveillance. Only a superior court judge can authorize electronic surveillance, and the legislative scheme sets a high standard for obtaining these authorizations. A judge must be satisfied that other investigative methods would fail, or have little likelihood of success, and that the granting of the authorization is in the best interest of the administration of justice. I share the approach of Martin J.A. in *R v Finlay and Grellette*, supra, at pp. 70 et seq., that this latter prerequisite imports as a minimum requirement that the issuing judge must be satisfied that there are reasonable and probable grounds to believe that an offence has been, or is being, committed and that the authorization sought will afford evidence of that offence. It can, I think, be seen that the provisions and safeguards of Part IV.1 of the Code have been designed to prevent the agencies of the state from intercepting private communications on the basis of mere suspicion.

In proceeding in this fashion, Parliament has, in my view, succeeded in striking an appropriate balance. It meets the high standard of the Charter which guarantees the right to be secure against unreasonable search and seizure by subjecting the power of the state to record our private communications to external restraint and requiring it to be justified by application of an objective criterion. The reason this represents an acceptable balance is that the imposition of an external and objective criterion affords a measure of protection to any citizen whose private communications have been intercepted. It becomes possible for the individual to call the state to account if he can establish that a given interception was not authorized in accordance with the requisite standard. If privacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself, a reasonable expectation of privacy would seem to demand that an individual may proceed on the assumption that the state may only violate this right by recording private communications on a clandestine basis when it has established to the satisfaction of a detached judicial officer that an offence has been or is being committed and that interception of private communications stands to afford evidence of the offence.

This, it seems to me, flows inexorably from the principles enunciated in *Hunter v Southam Inc.*, supra. In that case, this Court (p. 157) made the important point that the "assessment of the constitutionality of a search and seizure ... must focus on its `reasonable' or `unreasonable' impact on the subject of the search or the seizure, and not simply on its rationality in furthering some valid government objective". Applying this standard, it is fair to conclude that if the surreptitious recording of private communications is a search and seizure within the meaning of s. 8 of the Charter, it is because the law recognizes that a person's privacy is intruded on in an unreasonable manner whenever the state, without a prior showing of reasonable cause before a neutral judicial officer, arrogates to itself the right surreptitiously to record communications that the originator expects will not be intercepted by anyone other than the person intended by its originator to receive them, to use the language of the Code.

By contrast to the general provisions on electronic surveillance, the Code places no restriction on participant surveillance. The police may employ this practice in their absolute discretion, against whom they wish and for whatever reasons they wish, without any limit as to place or duration. There is a total absence of prior judicial supervision of this practice.

I am unable to see any logic to this distinction between third party electronic surveillance and participant surveillance. The question whether unauthorized electronic surveillance of private communications violates a reasonable expectation of privacy cannot, in my view, turn on the location of the hidden microphone. Whether the microphone is hidden in the wall or concealed on the body of a participant to the conversation, the assessment whether the surreptitious recording trenches on a reasonable expectation of privacy must turn on whether the person whose words were recorded spoke in circumstances in which it was reasonable for that person to expect that his or her words would only be heard by the persons he or she was addressing.

As I see it, where persons have reasonable grounds to believe their communications are private communications in the sense defined above, the unauthorized surreptitious electronic recording of those communications cannot fail to be perceived as an intrusion on a reasonable expectation of privacy.

The Charter standard just described must, in my view, apply on a uniform basis. To have any meaning, it must be taken to afford protection against the arbitrary recording of private communications every time we speak in the expectation that our words will only be heard by the person or persons to whom we direct our remarks. Section 8 of the Charter guarantees the right to be secure against unreasonable search or seizure. Our perception that we are protected against arbitrary interceptions of private communications ceases to have any real basis once it is accepted that the state is free to record private communications, without constraint, provided only that it has secured the agreement of one of the parties to the communication. Since we can never know if our listener is an informer, and since if he proves to be one, we are to be taken to be tacitly consenting to the risk that the state may be listening to and recording our conversations, we should be prepared to run this risk every time we speak. I conclude that the risk analysis relied on by the Court of Appeal, when taken to its logical conclusion, must destroy all expectations of privacy.

I am unable to see any similarity between the risk that someone will listen to one's words with the intention of repeating them and the risk involved when someone listens to them while simultaneously making a permanent electronic record of them. These risks are of a different order of magnitude. The one risk may, in the context of law enforcement, be viewed as a reasonable invasion of privacy, the other unreasonable. They involve different risks to the individual and the body politic. In other words, the law recognizes that we inherently have to bear the risk of the "tattletale" but draws the line at concluding that we must also bear, as the price of choosing to speak to another human being, the risk of having a permanent electronic recording made of our words.

The risk analysis relied on by the Court of Appeal fails to take due account of this key fact that our right under s. 8 of the Charter extends to a right to be free from unreasonable invasions of our right to privacy. The Court of Appeal was correct in stating that the expression of an idea and the assumption of the risk of disclosure are concomitant. However, it does not follow that, because in any conversation we run the risk that our interlocutor may in fact be bent on divulging our confidences, it is therefore constitutionally proper for the person to whom we speak to make a permanent electronic recording of that conversation. The Charter, it is accepted, proscribes the surreptitious recording by third parties of our private communications on the basis of mere suspicion alone. It would be strange indeed if, in the absence of a warrant requirement, instrumentalities of the state, through the medium of participant surveillance, were free to conduct just such random fishing expeditions in the hope of uncovering evidence of crime, or by the same token, to satisfy any curiosity they may have as to a person's views on any matter whatsoever.

In summary, the question whether to regulate participant surveillance cannot logically be made to turn on the expectations of individuals as to whether their interlocutor will betray their confidence. No justification for the arbitrary exercise of state power can be made to rest on the simple fact that persons often prove to be poor judges of whom to trust when divulging confidences or on the fact that the risk of divulgation is a given in the decision to speak to another human being. On the other hand, the question whether we should countenance participant surveillance has everything to do with the need to strike a fair balance between the right of the state to intrude on the private lives of its citizens and the right of those citizens to be left alone.

This is the manner in which the issue has been framed in the American appellate decisions that have rejected *United States v White*, supra, in interpreting rights to privacy in state constitutions. The reasoning in these decisions, in my respectful view, provides a complete answer to the view that the risk posed by the divulgation of the informer, and that posed by letting the agents of the state, at their whim, surreptitiously record private communications to which they are privy, are risks of the same order. These decisions make an eloquent case in support of the proposition that unregulated participant surveillance cannot be reconciled with the right to be secure against unreasonable search and seizure.

B. Offences in respect of which applications for interception may be made

10.3 It is noteworthy that the following offences are set out in the definition of "offence" in section 183 of the Canadian Criminal Code in respect of which applications for interceptions may be made namely-

> "offence" means an offence contrary to, any conspiracy or attempt to commit or being an accessory after the fact in relation to an offence contrary to, or any counselling in relation to an offence contrary to section 47 (high treason), 51 (intimidating Parliament or a legislature), 52 (sabotage), 57 (forgery, etc.), 61 (sedition), 76 (hijacking), 77 (endangering safety of aircraft or airport), 78 (offensive weapons, etc., on aircraft), 78.1 (offences against maritime navigation or fixed platforms), 80 (breach of duty), 81 (using explosives), 82 (possessing explosive), 90 (possession of prohibited weapon), 95 (importing or exporting of prohibited weapon), 119 (bribery, etc.), 120 (bribery, etc.), 121 (fraud on government), 122 (breach of trust), 123 (municipal corruption), 132 (perjury), 139 (obstructing justice), 144 (prison breach), 163.1 (child pornography), 184 (unlawful interception), 191 (possession of intercepting device), 235 (murder), 264.1 (uttering threats), 267 (assault with a weapon or causing bodily harm), 268 (aggravated assault), 269 (unlawfully causing bodily harm), 271 (sexual assault), 272 (sexual assault with a weapon, threats to a third party or causing bodily harm), 273 (aggravated sexual assault), 279 (kidnapping), 279.1 (hostage taking), 280 (abduction of person under sixteen), 281 (abduction of person under fourteen), 282 (abduction in contravention of custody order), 283 (abduction), 318 (advocating genocide), 327 (possession of device to obtain telecommunication facility or service), 334 (theft), 342 (theft, forgery, etc., of credit card), 342.1 (unauthorized use of computer), 342.2 (possession of device to obtain computer service), 344 (robbery), 346 (extortion), 347 (criminal interest rate), 348 (breaking and entering), 354 (possession of property obtained by crime), 356 (theft from mail), 367 (forgery), 368 (uttering forged document), 372 (false messages), 380 (fraud), 381 (using mails to defraud), 382 (fraudulent manipulation of stock exchange transactions), 424 (threat to commit offences against internationally protected person), 426 (secret commissions), 430 (mischief), 431 (attack on premises, residence or transport of internationally protected person), 433 (arson), 434 (arson), 434.1 (arson), 435 (arson for fraudulent purpose), 449 (making counterfeit money), 450 (possession, etc., of counterfeit money), 452 (uttering, etc., counterfeit money), 462.31 (laundering proceeds of crime) or 467.1 (participation in criminal organization), subsection 145(1) (escape, etc.), 201(1) (keeping gaming or betting house), 212(1) (procuring) or 462.33(11) (acting in contravention of restraint order), or paragraph 163(1)(a) (obscene materials), 202(1)(e) (pool-selling, etc.), section 5 (trafficking), 6 (importing and exporting), 7 (production), 8 (possession of property obtained by designated substance offences) or 9 (laundering proceeds of designated substance offences) of the Controlled Drugs and Substances Act, section 153 (false statements), 159 (smuggling), 163.1 (possession of property obtained by smuggling, etc.) or 163.2 (laundering proceeds of smuggling, etc.) of the Customs Act, sections 94.1 and 94.2 (organizing entry into Canada), 94.4 (disembarking persons at sea) and 94.5 (counselling false statements) of the Immigration Act, section 126.1 (possession of property obtained by excise offences), 126.2 (laundering proceeds of excise offences), 158 (unlawful distillation of spirits) or 163 (unlawful selling of spirits) or subsection 233(1) (unlawful packaging or stamping) or 240(1) (unlawful possession or sale of manufactured tobacco or cigars) of the Excise Act, section 198 (fraudulent bankruptcy) of the Bankruptcy and Insolvency Act, section 3 (spying) of the Official Secrets Act, section 13 (export or attempt to export), 14 (import or attempt to import), 15 (diversion, etc.), 16 (no transfer of permits), 17 (false information) or 18 (aiding and abetting) of the Export and Import Permits Act, or any other offence created by this Act for which an offender may be sentenced to imprisonment for five years or more that there are reasonable grounds to believe is part of a pattern of criminal activity planned and organized by a number of persons acting in concert or any other offence created by this or any other Act of Parliament for which an offender may be sentenced to

> imprisonment for five years or more that there are reasonable grounds to believe is committed for the benefit of, at the direction of or in association with a criminal organization;

10.4 The Canadian Law Reform Commission remarked in 1991 in its *Report Recodifying Criminal Procedure* that one of the most perplexing tasks, when trying to understand their wiretap legislation, is to discern an underlying principle justifying the long list of wiretappable offences.[3] They pointed out that in their Working Paper 47, while they accepted most of this list of crimes, they criticized and urged the deletion of the organized crime definition (ie "part of a pattern of criminal activity ...") on the ground that it adds little to the established definition of conspiracy, and that they recommended that some of the crimes be deleted from the list such as advocating genocide, while some new ones be added to it such as criminal interest rate. The Canadian Law Reform Commission explained that their recommendation contained in their Report was based on a simpler but equally sound policy dispensing with the need to adopt a long list of crimes, and that their proposed limit on the crimes for which a warrant may be obtained is largely adapted from their plan for the classification of crimes.[4]

C. Private communications and interception

10.5 As was noted in the introduction above, the Canadian legislation protects private communications against interceptions. The Canadian Criminal Code defines the term "private communication" as follows:

> "private communication" means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it;

10.6 Tremeear notes in his comment on the Canadian Criminal Code that the case of *R v*

---

3 At p 131.

4 They proposed the following provision:

> A judge may, on application, issue a warrant authorising the interception of a private communication by means of a surveillance device if the judge is satisfied that
>
> (a) there are reasonable grounds to believe that
>
> (i) a crime punishable by more than two years' imprisonment, or a conspiracy to commit, an attempt to commit, a furthering of or an attempted furthering of such a crime, has been or is being committed, and ...

Fegan makes it clear what private communications are.[5] The writer points out that this case noted that a digital number recorder (DNR) recording electronic impulses emitted from a monitored telephone on a computer printout tape which discloses the number dialled in an outgoing call, but not indicating whether the call is answered or the fact or substance of the communication, does not intercept a "private communication" in terms of the Part VI of the Criminal Code. It is also noted that a communication contemplates the exchange of information between persons, and that the initiation of a communication process by dialling a number does not constitute a communication, at least until the originator of the call is in a position to deliver the message. Tremeear also notes that the DNR only records the fact that a means of communication has been engaged but not the communication itself, and further that a communication in terms of section 183 does not embrace the action of an originator lifting a telephone receiver and dialling a number.

10.7 The Canadian Law Reform Commission proposed that the definition should read that "private communication" means any oral communication or any telecommunication made under circumstances in which it is reasonable for a party to it to expect that it will not be intercepted by a person other than a party to the communication, even if any party to it suspects that it is being intercepted by such a person. They noted that the then definition focussed on the expectation of the originator of a private communication that the communication will not be listened to by any person other than the intended recipient, and that the definition has created problems, since its effect is to break a conversation between two people into a series of private communications. The Canadian Law Reform Commission considered that their recommended definition avoids the somewhat artificial distinction, and in stead of referring to the reasonable expectation of privacy of the originator of the communication, it makes a communication private if it is made under circumstances in which it is reasonable for a party to expect that it will not be intercepted by someone other than a party. They were further of the view that the effect of the provision is to clarify that a private communication means not the individual statements that together make up a conversation, but the conversation as a whole. The Canadian Law Reform Commission considered that the clause more clearly adopts an objective test to determine if the communication is private. They were of the view that despite the reference in the definition to the originator's reasonable expectancy of privacy, the case law focuses initially on the originator's subjective expectation of privacy, and that the person must be found to have a

---

5 *Tremeear's Criminal Code* at p 295.

subjective expectation of privacy before a determination may be made as to whether that expectation is objectively reasonable. They noted that this raises the issue of whether a suspicion, held by one party to a private communication, that the communication is being intercepted should be allowed to defeat any claim to a reasonable expectation of privacy. They considered that the danger in requiring a subjective expectation of privacy as an initial threshold to be met is that it permits the subjective fears of a person to erode any reasonable expectation of privacy. The Canadian Law Reform Commission noted that if the government were, for example, to announce the following date that it would monitor all private communications to discover who intended to commit crimes, it would then be possible to argue that no one could reasonably expect that telephone conversations are private. They therefore noted that to prevent such a result, their proposed interpretation clause provides that a reasonable expectation of privacy is not made unreasonable "even if one party to the communication suspects that the communication is being intercepted".

D. Consent to intercept

10.8 Section 183.1 of the Canadian Criminal Code sets out who may consent to the interception of private communications. It provides that where a private communication is originated by more than one person or is intended by the originator thereof to be received by more than one person, a consent to the interception thereof by any one of those persons is sufficient consent for the purposes of any provision of Part VI of the Criminal Code.

E. The general rule prohibiting interception

10.9 The Criminal Code provides in section 184. (1) that every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.[6] Subsection (2) provides that subsection (1) does not apply, to-

---

6 The corresponding provisions regarding radio-based telephone communications provide as follows:

184.5 (1) Every person who intercepts, by means of any electro-magnetic, acoustic, mechanical or other device, maliciously or for gain, a radio-based telephone communication, if the originator of the communication or the person intended by the originator of the communication to receive it is in Canada, is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

(2) Section 183.1, subsection 184(2) and sections 184.1 to 190 and 194 to 196 apply, with

(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;

(b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;

(c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

(i) if the interception is necessary for the purpose of providing the service,

(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or

(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service; or

(d) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission.

F. Interception to prevent bodily harm

10.10 The Canadian Law Reform Commission noted that in the cases of *Duarte* (noted in the introduction above) and *Wiggens,* the Supreme Court of Canada rejected consent interceptions of private communications made in the absence of a prior judicial warrant, and that according to the Court, the surreptitious recording by the state of a person's private communications is an unjustifiable invasion of privacy. The Commission pointed out that in both cases the avowed purpose of the surreptitious interceptions was to obtain reliable evidence of the commission of a crime.[7] They further pointed out that the Criminal Code provided for a course of action whereby, if a surreptitious interception of a private communication was made by a party at the behest of the police, there was no need to go before a judge to obtain authorization to wiretap and that this meant that the police had a largely unfettered discretion as to how and when to intercept.[8] The Canadian Law Reform Commission explained that the cases of *R v Duarte* and

---

such modifications as the circumstances require, to interceptions of radio-based telephone communications referred to in subsection (1).

7 *Report Recodifying Criminal Procedure* at p 125.

8 *Report Recodifying Criminal Procedure* at p 124.

*R v Wiggens*held found that the simple consent of one party to the interception of his or her private communications cannot serve as a device for bypassing the need to obtain prior judicial approval in the form of an authorization, and that failure to obtain the necessary authorization constitutes unreasonable search and seizure under section 8 of the Canadian Charter. The Canadian Law Reform Commission pointed out that the Supreme Court did not consider in the cases before it the possibility that it might on occasion prove necessary to listen to private communications, not for evidentiary purposes, but in order to protect the life or safety of an undercover peace officer or an informer. They explained that this might occur, for example, where a peace officer is working undercover to investigate the activities of drug traffickers and a meeting is suddenly arranged between the officer and the traffickers, and that this is a highly dangerous circumstance that might emerge without sufficient time to arrange for the obtaining of a judicial warrant. They stated that in their view, in such emergency circumstances, legitimate concern for the peace officer's safety should preclude the need to obtain a warrant, in order to monitor for protective reasons the conversations between the undercover operative and the drug traffickers. They however also pointed out their proposed provision is carefully drafted to be consistent with the concern for privacy expressed by the Supreme Court,[9] and therefore their proposed authority to intercept was restricted to one kind of interception only, namely that of listening to the private communication. The Canadian Law Reform Commission considered that to record such a communication, a warrant should be required, since the purpose of recording communications is evidentiary and not protective.

10.11 The Canadian Criminal Code provides presently in section 184.1 (1) that an agent of the state may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication if -

(a) either the originator of the private communication or the person intended by the originator to receive it has consented to the interception;
(b) the agent of the state believes on reasonable grounds that there is a risk of bodily harm to the person who consented to the interception; and
(c) the purpose of the interception is to prevent the bodily harm.

10.12 Section 184.2 of the Code regulates the admissibility of intercepted communications in

---

9 They proposed the following clause:
A peace officer may, without a warrant, use a surveillance device to listen to but not record a private communication to which a peace officer or agent of a peace officer is a party if it is reasonable to believe that the life or safety of the officer or agent may be in danger.

regard of which no prior authorization was obtained, as follows:

> (2) The contents of a private communication that is obtained from an interception pursuant to subsection (1) are inadmissible as evidence except for the purposes of proceedings in which actual, attempted or threatened bodily harm is alleged, including proceedings in respect of an application for an authorization under this Part or in respect of a search warrant or a warrant for the arrest of any person.

10.13 Section 184.3 provides that the agent of the state[10] who intercepts a private communication pursuant to subsection (1) shall, as soon as is practicable in the circumstances, destroy any recording of the private communication that is obtained from an interception pursuant to subsection (1), any full or partial transcript of the recording and any notes made by that agent of the private communication if nothing in the private communication suggests that bodily harm, attempted bodily harm or threatened bodily harm has occurred or is likely to occur.

G. Interception with consent and applications for authorization

10.14 Section 184.2 (1) of the Criminal Code provides that a person may intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where either the originator of the private communication or the person intended by the originator to receive it has consented to the interception and an authorization has been obtained pursuant to subsection (3). Subsection (2) provides that an application for an authorization under the section must be made by a peace officer, or a public officer who has been appointed or designated to administer or enforce any federal or provincial law and whose duties include the enforcement of the Act or any other Act of Parliament, ex parte and in writing to a provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552, and must be accompanied by an affidavit, which may be sworn on the information and belief of that peace officer or public officer or of any other peace officer or public officer, deposing to the following matters:

(a) that there are reasonable grounds to believe that an offence against the or any other Act of Parliament has been or will be committed;
(b) the particulars of the offence;

---

10 Agent of the State is defined as follows in section 184.4 of the Criminal Code:
(4) For the purposes of this section, "agent of the state" means
(a) a peace officer; and (b) a person acting under the authority of, or in cooperation with, a peace officer.

(c) the name of the person who has consented to the interception;
(d) the period for which the authorization is requested; and
(e) in the case of an application for an authorization where an authorization has previously been granted under the section or section 186, the particulars of the authorization.

10.15 Section 184.3 of the Criminal Code presently sets out the criteria to be applied by the judge in deciding whether an authorisation should be granted:

> An authorization may be given under this section if the judge to whom the application is made is satisfied that
> (a) there are reasonable grounds to believe that an offence against the Act or any other Act of Parliament has been or will be committed;
> (b) either the originator of the private communication or the person intended by the originator to receive it has consented to the interception; and
> (c) there are reasonable grounds to believe that information concerning the offence referred to in paragraph (a) will be obtained through the interception sought.[11]

10.16 Section 184.4 prescribes the content and limitation of the authorization and provides that an authorization given under the section shall-

(a) state the offence in respect of which private communications may be intercepted;
(b) state the type of private communication that may be intercepted;
(c) state the identity of the persons, if known, whose private communications are to be intercepted, generally describe the place at which private communications may be intercepted, if a general description of that place can be given, and generally describe the manner of interception that may be used;
(d) contain the terms and conditions that the judge considers advisable in the public interest; and
(e) be valid for the period, not exceeding sixty days, set out therein.

---

11 The following wording was proposed by the Canadian Law Reform Commission in this regard: (See *Report Recodifying Criminal Procedure* at p 132.)
(a) there are reasonable grounds to believe that
(i) ...;
(ii)the interception of the private communication will assist in the investigation of the crime;
The Canadian Law Reform Commission noted the case of *R v Finlay and Grelette* (1985) 48 CR (3d) 341 (Ont CA) where the court held that the provision then contained in the Criminal Code "imports 'at least' the American Title III standard of 'reasonable ground [probable cause] to believe that communications concerning the particular offence will be obtained through the interception sought, a standard that he appeared to equate with the 'will assist' standard.

H. Application by means of telecommunication

10.17 An application for an authorization may be made ex parte to a provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552, by telephone or other means of telecommunication, if it would be impracticable in the circumstances for the applicant to appear personally before a judge.[12] Such an application must be on oath and must be accompanied by a statement that includes the matters referred to in paragraphs 184.2(2)(a) to (e) of the Code[13] and must state the circumstances that make it impracticable for the applicant to appear personally before a judge.

10.18 The judge must record, in writing or otherwise, the application for an authorization made and, on determination of the application, must cause the writing or recording to be placed in the packet referred to in subsection 187(1) and sealed in that packet, and a recording sealed in a packet is treated as if it were a document for the purposes of section 187.[14] The oath concerned may be administered by telephone or other means of telecommunication.[15] An applicant who uses a means of telecommunication that produces writing may, instead of swearing an oath, make a statement in writing stating that all matters contained in the application are true to the knowledge or belief of the applicant and such a statement is deemed to be a statement made under oath.[16]

10.19 Where the judge to whom an application is made is satisfied that the circumstances referred to in paragraphs 184.2(3)(a) to (c) exist and that the circumstances make it impracticable for the applicant to appear personally before a judge, the judge may, on such terms and conditions, if any, as are considered advisable, give an authorization by telephone

---

12 Section 184.3 (1) of the Criminal Code.

13 Namely-
- (a) that there are reasonable grounds to believe that an offence against the or any other Act of Parliament has been or will be committed;
- (b) the particulars of the offence;
- (c) the name of the person who has consented to the interception;
- (d) the period for which the authorization is requested; and
- (e) in the case of an application for an authorization where an authorization has previously been granted under the section or section 186, the particulars of the authorization.

14 Section 184.3(3) of the Criminal Code.

15 Section 184.3(4) of the Criminal Code.

16 Section 184.3(5).

or other means of telecommunication for a period of up to thirty-six hours.[17] Where a judge gives an authorization by telephone or other means of telecommunication, other than a means of telecommunication that produces a writing, the judge must complete and sign the authorization in writing, noting on its face the time, date and place at which it is given.[18] The applicant concerned must, on the direction of the judge, complete a facsimile of the authorization in writing, noting on its face the name of the judge who gave it and the time, date and place at which it was given,[19] and the judge must, as soon as is practicable after the authorization has been given, cause the authorization to be placed in the packet referred to in subsection 187(1) and sealed in that packet.

10.20 Where a judge gives an authorization by a means of telecommunication that produces writing, the judge must complete and sign the authorization in writing, noting on its face the time, date and place at which it is given; transmit the authorization by the means of telecommunication to the applicant, and the copy received by the applicant shall be deemed to be a facsimile referred to in paragraph (7)(b); and as soon as is practicable after the authorization has been given, cause the authorization to be placed in the packet referred to in subsection 187(1) and sealed in that packet.

I. Interception in exceptional circumstances without authorization

10.21 The Criminal Code makes also provision for unauthorized interception by a peace officer[20] which the author Tremeear points out is bound to attract scrutiny on constitutional grounds. A peace officer may therefore intercept, by means of any electro-magnetic, acoustic, mechanical or other device, a private communication where-

(a) the peace officer believes on reasonable grounds that the urgency of the situation is such that an authorization could not, with reasonable diligence, be obtained under any other provision of Part VI of the Criminal Code;
(b) the peace officer believes on reasonable grounds that such an interception is immediately necessary to prevent an unlawful act that would cause serious harm to any person or to property; and
(c) either the originator of the private communication or the person intended by the originator

---

17 Section 184.3(6).

18 Section 184.3(7)(a).

19 Section 184.3(7)(b).

20 Section 184.4.

to receive it is the person who would perform the act that is likely to cause the harm or is the victim, or intended victim, of the harm.

J. Applications for authorization

10.22 The Criminal Code defines in section 185 the basis upon which applications may be made for conventional judicial authorization (which lasts 60 days) to intercept communications and for extension of the period within which notice of interception must be given to the object thereof. An application for an authorization must be made ex parte and in writing to a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 and must be signed by the Attorney General of the province in which the application is made or the Solicitor General of Canada or an agent specially designated in writing for the purposes of this section by-

(a) the Solicitor General of Canada personally or the Deputy Solicitor General of Canada personally, if the offence under investigation is one in respect of which proceedings, if any, may be instituted at the instance of the Government of Canada and conducted by or on behalf of the Attorney General of Canada, or

(b) the Attorney General of a province personally or the Deputy Attorney General of a province personally, in any other case,

and must be accompanied by an affidavit, which may be sworn on the information and belief of a peace officer or public officer deposing to the following matters:[21]

---

21 The Canadian Law Reform Commission proposed that an application for a warrant should be made unilaterally, in person and in private, orally or in writing, to a judge of the province in which the communication is to be intercepted, and that the application must disclose the following particulars-

(a) the applicants' name;
(b) the date and place the application is made;
(c) the crime under investigation, and the facts and circumstances of that crime and their seriousness;
(d) the type of private communication to be intercepted;
(e) a general description of the means of interception to be used;
(f) the names of all persons whose private communications are to be intercepted or, if the names cannot be ascertained, a description or other means of identifying those persons individually or, if that is not possible, the class of those unidentified persons;
(g) the places, if known, at which the interception would occur;
(h) whether any privileged communications are likely to be intercepted;
(i) the grounds for believing that the interception may assist in the investigation of the crime;
(j) the period for which the warrant is requested;
(k) any other investigative method that has been tried without success or, if no other method has been tried, the reasons why no other method is likely to succeed or why the urgency is such that no other method is practicable;
(l) a list of any previous applications for a warrant in respect of the same crime and the same persons or class of persons indicating the date each application was made, the name of the judge who heard each application and whether each application was withdrawn, refused or granted;

(c) the facts relied on to justify the belief that an authorization should be given together with particulars of the offence,
(d) the type of private communication proposed to be intercepted,
(e) the names, addresses and occupations, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used,
(f) the number of instances, if any, on which an application has been made under this section in relation to the offence and a person named in the affidavit pursuant to paragraph (e) and on which the application was withdrawn or no authorization was given, the date on which each application was made and the name of the judge to whom each application was made,
(g) the period for which the authorization is requested, and
(h) whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.[22]

10.23 Sections 185(2) to (4) permit an application to be accompanied by an application to substitute for the statutory period of section 196(1) of 90 days a longer period, not exceeding three years. The application must be personally signed by the Attorney General or Solicitor General of Canada, as the case may be, and must be considered first, prior to any determination of the application for authorization. The judge to whom the applications are made is to consider the affidavit filed in support of the application for the authorization and any other affidavits submitted in support of the application for deferral of notification. The criterion to be applied is whether the interests of justice warrant the granting of the application. Where the application for deferral of notice is refused, or a period fixed less than that requested in the application, the applicant may withdraw the application for the authorization and thereupon the judge shall not proceed to determine it. Both application must then be returned to the applicant. Where an application for deferral of notification is successful, a period, not exceeding three

---

(m) if the applicant requests authority to make a surreptitious entry to install, service or remove a surveillance device,
  (i) why the entry is required and why other less intrusive means of installation, service or removal are unlikely to be effective, and
  (ii) the place where the entry would be made; and
(n) if the applicant requests an assistance order referred to in section 139, the nature of the assistance required.

22 Section 185.(1.1) however provides that notwithstanding paragraph (1)(h), that paragraph does not apply where the application for an authorization is in relation to (a) an offence under section 467.1; or (b) an offence committed for the benefit of, at the direction of or in association with a criminal organization.

years, is fixed in the order in substitution for the statutory period of section 196(1).

10.24 Section 186. (1) of the Criminal Code sets out the basis upon which and form in which conventional authorizations and renewals thereof may be granted. It provides that an authorization may be given if the judge to whom the application is made is satisfied that it would be in the best interests of the administration of justice to do so, and that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.[23] The Code further provides in section 186(2) that no authorization may be given to intercept a private communication at the office or residence of a solicitor, or at any other place ordinarily used by a solicitor and by other solicitors for the purpose of consultation with clients, unless the judge to whom the application is made is satisfied that there are reasonable grounds to believe that the solicitor, any other solicitor practising with him, any person employed by him or any other such solicitor or a member of the solicitor's household has been or is about to become a party to an offence. The Code also sets out that where an authorization is given in relation to the interception of private communications at a place described in subsection (2), the judge by whom the authorization is given shall include therein such terms and conditions as he or she considers advisable to protect privileged communications between solicitors and clients.

10.25 Section 186.(4) of the Criminal Code prescribes the particulars to be contained in an authorization and provides that an authorization shall-

(a) state the offence in respect of which private communications may be intercepted;
(b) state the type of private communication that may be intercepted;
(c) state the identity of the persons, if known, whose private communications are to be intercepted, generally describe the place at which private communications may be intercepted, if a general description of that place can be given[24], and

---

23 Section 186(1.1) provides that notwithstanding paragraph (1)(b), that paragraph does not apply where the judge is satisfied that the application for an authorization is in relation to (a) an offence under section 467.1; or (b) an offence committed for the benefit of, at the direction of or in association with a criminal organization.

24 In R. v. Thompson [1990] 2 S.C.R. 1111 the court held as follows:
However, while the nature of the invasion of a person's privacy is constant, what changes with that person's location is the possible effect on third parties. Where the police are aware, prior to seeking an authorization, that the targets make extensive use of pay telephones, the

generally describe the manner of interception that may be used;

(d) contain such terms and conditions as the judge considers advisable in the public interest; and

(e) be valid for the period, not exceeding sixty days, set out therein.

10.26 The Code provides that the Solicitor General of Canada or the Attorney General, as the case may be, may designate a person or persons who may intercept private communications under authorizations.[25] Section 186.(6) contains the requirements for renewals of authorization stating that renewals of an authorization may be given by a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 on receipt by him of an ex parte application in writing signed by the Attorney General of the province in which the application is made or the Solicitor General of Canada or an agent specially designated in writing for the purposes of section 185 by the Solicitor General of Canada or the Attorney General, as the case may be, accompanied by an affidavit of a peace officer or public officer deposing to the following matters:

(a) the reason and period for which the renewal is required,

(b) full particulars, together with times and dates, when interceptions, if any, were made or attempted under the authorization, and any information that has been obtained by any interception, and

(c) the number of instances, if any, on which, to the knowledge and belief of the deponent, an application has been made under this subsection in relation to the same authorization and on which the application was withdrawn or no renewal was given, the date on which each application was made and the name of the judge to whom each application was made,

and supported by such other information as the judge may require.

10.27 A renewal of an authorization may be given if the judge to whom the application is made is satisfied that any of the circumstances described in subsection (1) still obtain, but no renewal shall be for a period exceeding sixty days. The Criminal Code also provides for a time limitation in relation to criminal organizations by providing in section 186.(1.1) that notwithstanding

---

authorizations, to comply with s. 8, must at a minimum provide that conversations at a pay telephone should not be intercepted unless there are reasonable and probable grounds for believing that a target is using the telephone at the time that the listening device is activated. The police cannot simply install a listening device and leave it running indiscriminately in hope that a target may come along. While the failure to impose conditions protecting the public interest under s. 178.13(2)(d) of the Code is not unlawful because the power is discretionary, the failure to do so in the present circumstances was unreasonable. Therefore, any evidence obtained as a result of interceptions at pay telephones in the absence of reasonable and probable grounds for believing that a target was using the telephone was obtained in contravention of s. 8.

25 Section 186.(5).

paragraphs 184.2(4)(e) and 186(4)(e) and subsection 186(7), an authorization or any renewal of an authorization may be valid for one or more periods specified in the authorization exceeding sixty days, each not exceeding one year, where the authorization is in relation to-

(a) an offence under section 467.1; or
(b) an offence committed for the benefit of, at the direction of or in association with a criminal organization.

K. Manner in which application to be kept secret

10.28 The Criminal Code provides in section 187.(1) that all documents relating to an application made pursuant to any provision of Part VI of the Code are confidential and, subject to subsection (1.1), shall be placed in a packet and sealed by the judge to whom the application is made immediately on determination of the application, and that packet shall be kept in the custody of the court in a place to which the public has no access or in such other place as the judge may authorize and shall not be dealt with except in accordance with subsections (1.2) to (1.5). Subsections (1.2) to (1.5) set the procedure in regard to sealed packets out as follows:

(1.1) An authorization given under this Part need not be placed in the packet except where, pursuant to subsection 184.3(7) or (8), the original authorization is in the hands of the judge, in which case that judge must place it in the packet and the facsimile remains with the applicant.
(1.2) The sealed packet may be opened and its contents removed for the purpose of dealing with an application for a further authorization or with an application for renewal of an authorization.
(1.3) A provincial court judge, a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 may order that the sealed packet be opened and its contents removed for the purpose of copying and examining the documents contained in the packet.
(1.4) A judge or provincial court judge before whom a trial is to be held and who has jurisdiction in the province in which an authorization was given may order that the sealed packet be opened and its contents removed for the purpose of copying and examining the documents contained in the packet if
  (a) any matter relevant to the authorization or any evidence obtained pursuant to the authorization is in issue in the trial; and
  (b) the accused applies for such an order for the purpose of consulting the documents to prepare for trial.
(1.5) Where a sealed packet is opened, its contents shall not be destroyed except pursuant to an order of a judge of the same court as the judge who gave the authorization.

10.29 In terms of section 186.(2) an order under subsection (1.2), (1.3), (1.4) or (1.5) made

with respect to documents relating to an application made pursuant to section 185 or subsection 186(6) or 196(2) may only be made after the Attorney General or the Solicitor General by whom or on whose authority the application for the authorization to which the order relates was made has been given an opportunity to be heard. Section 186.(3) provides likewise that an order under subsection (1.2), (1.3), (1.4) or (1.5) made with respect to documents relating to an application made pursuant to subsection 184.2(2) or section 184.3 may only be made after the Attorney General has been given an opportunity to be heard.

10.30 The Criminal Code provides in section 186.(4) for the editing of copies of documents by the prosecutor. Under this subsection where a prosecution has been commenced and an accused applies for an order for the copying and examination of documents pursuant to subsection (1.3) or (1.4), the judge shall not, notwithstanding those subsections, provide any copy of any document to the accused until the prosecutor has deleted any part of the copy of the document that the prosecutor believes would be prejudicial to the public interest, including any part that the prosecutor believes could-

(a) compromise the identity of any confidential informant;
(b) compromise the nature and extent of ongoing investigations;
(c) endanger persons engaged in particular intelligence-gathering techniques and thereby prejudice future investigations in which similar techniques would be used; or
(d) prejudice the interests of innocent persons.

10.31 After the prosecutor has deleted the parts of the copy of the document to be given to the accused under subsection (4), the accused must be provided with an edited copy of the document.[26] After the accused has received an edited copy of a document, the prosecutor must keep a copy of the original document, and an edited copy of the document and the original document must be returned to the packet and the packet resealed.[27] An accused to whom an edited copy of a document has been provided pursuant to subsection (5) may request that the judge before whom the trial is to be held order that any part of the document deleted by the prosecutor be made available to the accused, and the judge must order that a copy of any part that, in the opinion of the judge, is required in order for the accused to make full answer and defence and for which the provision of a judicial summary would not be sufficient, be made

---

26 Section 186.(5).

27 Section 186.(6).

available to the accused.

L. Applications to specially appointed judges in emergency

10.32 In terms of section 188. (1) if the urgency of the situation requires interception of private communications to commence before an authorization could, with reasonable diligence, be obtained under section 186, an ex parte application may be made to a judge of a superior court of criminal jurisdiction, or a judge as defined in section 552, designated from time to time by the Chief Justice. Such an application must be made by a peace officer specially designated in writing, by name or otherwise, by the Solicitor General of Canada, if the offence is one in respect of which proceedings, if any, may be instituted by the Government of Canada and conducted by or on behalf of the Attorney General of Canada, or the Attorney General of a province, in respect of any other offence in the province. Under section 188.(2) where the judge to whom an application is made pursuant to subsection (1) is satisfied that the urgency of the situation requires that interception of private communications commence before an authorization could, with reasonable diligence, be obtained under section 186, he may, on such terms and conditions, if any, as he considers advisable, give an authorization in writing for a period of up to thirty-six hours. The Criminal Code also governs the admissibility of evidence obtained under an emergency application. Section 188.(5) provides that the trial judge may deem inadmissible the evidence obtained by means of an interception of a private communication pursuant to a subsequent authorization given under section 188, where he finds that the application for the subsequent authorization was based on the same facts, and involved the interception of the private communications of the same person or persons, or related to the same offence, on which the application for the original authorization was based.

M. Executions of authorizations

10.33 The Criminal Code also makes provision for the execution of authorizations by setting out in section 188.1(1) that subject to subsection (2), the interception of a private communication authorized pursuant to section 184.2, 184.3, 186 or 188 may be carried out anywhere in Canada. Under section 188.(2) where an authorization is given under section 184.2, 184.3, 186 or 188 in one province but it may reasonably be expected that it is to be executed in another province and the execution of the authorization would require entry into or upon the property of any person in the other province or would require that an order under

section 487.02 be made with respect to any person in that other province, a judge in the other province may, on application, confirm the authorization and when the authorization is so confirmed, it shall have full force and effect in that other province as though it had originally been given in that other province.

N. Notice of intention to produce evidence

10.34 The Canadian Criminal Code provides that notice must be given by the party intending to adduce evidence in regard to an intercepted communication. Under section 189.(5) the contents of a private communication that is obtained from an interception of the private communication pursuant to any provision of, or pursuant to an authorization given under Part VI of the Criminal Code shall not be received in evidence unless the party intending to adduce it has given to the accused reasonable notice of the intention together with-

(a) a transcript of the private communication, where it will be adduced in the form of a recording, or a statement setting out full particulars of the private communication, where evidence of the private communication will be given viva voce; and
(b) a statement respecting the time, place and date of the private communication and the parties thereto, if known.

10.35 Tremeear notes the case of *R v Commisso*[28] in which the court found that once the judge has authorized the interception of a conversation, evidence in support of any criminal offence incidentally disclosed is admissible, even though the authorisation did not specifically authorize an interception for that offence and, assuming no material non-disclosure, whether or not the offence was anticipated or unanticipated.

O. Privilege

10.36 The Criminal Code provides on the issue of privileged that any information obtained by an interception that, but for the interception, would have been privileged remains privileged and inadmissible as evidence without the consent of the person enjoying the privilege.[29]

---

28 (1983) 36 CR (3d) 105.

29 Section 188.(6).

P. Further particulars

10.37 Under section 190 of the criminal Code where an accused has been given notice pursuant to subsection 189(5), any judge of the court in which the trial of the accused is being or is to be held may at any time order that further particulars be given of the private communication that is intended to be adduced in evidence.

Q. Possession, sale or purchase of any electro-magnetic, acoustic, mechanical or other device or any component etc.

10.38 In terms of section 191.(1) every one who possesses, sells or purchases any electro-magnetic, acoustic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communications is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years. The Criminal Code makes provision in section 191(2) for the following exceptions by providing that subsection (1) does not apply to-

(a) a police officer or police constable in possession of a device or component described in subsection (1) in the course of his employment;
(b) a person in possession of such a device or component for the purpose of using it in an interception made or to be made in accordance with an authorization;
(b.1) a person in possession of such a device or component under the direction of a police officer or police constable in order to assist that officer or constable in the course of his duties as a police officer or police constable;
(c) an officer or a servant of Her Majesty in right of Canada or a member of the Canadian Forces in possession of such a device or component in the course of his duties as such an officer, servant or member, as the case may be; and
(d) any other person in possession of such a device or component under the authority of a licence issued by the Solicitor General of Canada.

10.39 The Criminal Code also prescribes the terms and conditions of licence by providing in section 199.(3) that a licence issued for the purpose of paragraph (2)(d) may contain such terms and conditions relating to the possession, sale or purchase of a device or component described in subsection (1) as the Solicitor General of Canada may prescribe. Under section 192.(1) where a person is convicted of an offence under section 184 or 191, any electro-magnetic, acoustic, mechanical or other device by means of which the offence was committed or the possession of which constituted the offence, on the conviction, in addition to any punishment that is imposed, may be ordered forfeited to Her Majesty whereupon it may be

disposed of as the Attorney General directs. Furthermore, section 192(2) provides that no order for forfeiture shall be made under subsection (1) in respect of telephone, telegraph or other communication facilities or equipment owned by a person engaged in providing telephone, telegraph or other communication service to the public or forming part of the telephone, telegraph or other communication service or system of that person by means of which an offence under section 184 has been committed if that person was not a party to the offence.

R. Disclosure of information

10.40 The Criminal Code also governs the disclosure of information in section 193 and provides that where a private communication has been intercepted by means of an electro-magnetic, acoustic, mechanical or other device without the consent, express or implied, of the originator thereof or of the person intended by the originator thereof to receive it, every one who, without the express consent of the originator thereof or of the person intended by the originator thereof to receive it,

(a) wilfully uses or discloses the private communication or any part thereof or the substance, meaning or purport thereof or of any part thereof, or
(b) discloses the existence thereof, is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.[30]

The Code however provides in section 193(2) that subsection (1) does not apply to a person who discloses a private communication or any part thereof or the substance, meaning or purport thereof or of any part thereof or who discloses the existence of a private communication-

(a) in the course of or for the purpose of giving evidence in any civil or criminal

---

30 Section 193.1(1) contains a corresponding provision on the disclosure of information received from interception of radio-based telephone communications and provides as follows:
Every person who wilfully uses or discloses a radio-based telephone communication or who wilfully discloses the existence of such a communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years, if
(a) the originator of the communication or the person intended by the originator of the communication to receive it was in Canada when the communication was made;
(b) the communication was intercepted by means of an electromagnetic, acoustic, mechanical or other device without the consent, express or implied, of the originator of the communication or of the person intended by the originator to receive the communication; and
(c) the person does not have the express or implied consent of the originator of the communication or of the person intended by the originator to receive the communication.
(2) Subsections 193(2) and (3) apply, with such modifications as the circumstances require, to disclosures of radio-based telephone communications.

proceedings or in any other proceedings in which the person may be required to give evidence on oath;

(b) in the course of or for the purpose of any criminal investigation if the private communication was lawfully intercepted;

(c) in giving notice under section 189 or furnishing further particulars pursuant to an order under section 190;

(d) in the course of the operation of

(i) a telephone, telegraph or other communication service to the public, or

(ii) a department or an agency of the Government of Canada,

if the disclosure is necessarily incidental to an interception described in paragraph 184(2)(c) or (d);

(e) where disclosure is made to a peace officer or prosecutor in Canada or to a person or authority with responsibility in a foreign state for the investigation or prosecution of offences and is intended to be in the interests of the administration of justice in Canada or elsewhere; or

(f) where the disclosure is made to the Director of the Canadian Security Intelligence Service or to an employee of the Service for the purpose of enabling the Service to perform its duties and functions under section 12 of the Canadian Security Intelligence Service Act.

10.41 In terms of section 193.(3) subsection (1) does not apply to a person who discloses a private communication or any part thereof or the substance, meaning or purport thereof or of any part thereof or who discloses the existence of a private communication where that which is disclosed by him was, prior to the disclosure, lawfully disclosed in the course of or for the purpose of giving evidence in proceedings referred to in paragraph (2)(a).

S. Damages

10.42 The Criminal Code makes also provision that subject to subsection (2), a court that convicts an accused of an offence under section 184, 184.5, 193 or 193.1 may, on the application of a person aggrieved, at the time sentence is imposed, order the accused to pay to that person an amount not exceeding five thousand dollars as punitive damages.[31] However, no amount shall be ordered to be paid under subsection (1) to a person who has commenced an action under Part II of the Crown Liability Act.[32] Where an amount that is ordered to be paid under section 194.(1) is not paid forthwith, the applicant may, by filing the order, enter as a judgment, in the superior court of the province in which the trial was held, the amount ordered to be paid, and that judgment is enforceable against the accused in the same manner as if it

---

31 Section 194.(1).

32 Section 194.(2).

were a judgment rendered against the accused in that court in civil proceedings.[33] All or any part of an amount that is ordered to be paid under section 194.(1) may be taken out of moneys found in the possession of the accused at the time of his arrest, except where there is a dispute respecting ownership of or right of possession to those moneys by claimants other than the accused.

T. Annual report

10.43 The Criminal Code also prescribes the preparation of an annual report by the Solicitor General of Canada to be Tabled in Parliament as well as the preparation and publishing to the public of annual reports by the Attorneys General of the provinces. In terms of section 195.(1) of the Criminal Code the Solicitor General of Canada shall, as soon as possible after the end of each year, prepare a report relating to-

(a) authorizations for which he and agents to be named in the report who were specially designated in writing by him for the purposes of section 185 made application, and

(b) authorizations given under section 188 for which peace officers to be named in the report who were specially designated by him for the purposes of that section made application,

and interceptions made thereunder in the immediately preceding year. Under subsection (2) the report referred to in subsection (1) shall, in relation to authorizations and interceptions made thereunder, set out-

(a) the number of applications made for authorizations;

(b) the number of applications made for renewal of authorizations;

(c) the number of applications referred to in paragraphs (a) and (b) that were granted, the number of those applications that were refused and the number of applications referred to in paragraph (a) that were granted subject to terms and conditions;

(d) the number of persons identified in an authorization against whom proceedings

---

33 Section 194.(3).

were commenced at the instance of the Attorney General of Canada in respect of-

(i) an offence specified in the authorization,

(ii) an offence other than an offence specified in the authorization but in respect of which an authorization may be given, and

(iii) an offence in respect of which an authorization may not be given;

(e) the number of persons not identified in an authorization against whom proceedings were commenced at the instance of the Attorney General of Canada in respect of

(i) an offence specified in such an authorization,

(ii) an offence other than an offence specified in such an authorization but in respect of which an authorization may be given, and

(iii) an offence other than an offence specified in such an authorization and for which no such authorization may be given,

and whose commission or alleged commission of the offence became known to a peace officer as a result of an interception of a private communication under an authorization;

(f) the average period for which authorizations were given and for which renewals thereof were granted;

(g) the number of authorizations that, by virtue of one or more renewals thereof, were valid for more than sixty days, for more than one hundred and twenty days, for more than one hundred and eighty days and for more than two hundred and forty days;

(h) the number of notifications given pursuant to section 196;

(i) the offences in respect of which authorizations were given, specifying the number of authorizations given in respect of each of those offences;

(j) a description of all classes of places specified in authorizations and the number of authorizations in which each of those classes of places was specified;

(k) a general description of the methods of interception involved in each interception under an authorization;

(l) the number of persons arrested whose identity became known to a peace officer as a result of an interception under an authorization;

(m) the number of criminal proceedings commenced at the instance of the Attorney General of Canada in which private communications obtained by interception

under an authorization were adduced in evidence and the number of those proceedings that resulted in a conviction; and

(n) the number of criminal investigations in which information obtained as a result of the interception of a private communication under an authorization was used although the private communication was not adduced in evidence in criminal proceedings commenced at the instance of the Attorney General of Canada as a result of the investigations.

10.44 In terms of section 195.(3) the report referred to in subsection (1) shall, in addition to the information referred to in subsection (2), set out-

(a) the number of prosecutions commenced against officers or servants of Her Majesty in right of Canada or members of the Canadian Forces for offences under section 184 or 193; and

(b) a general assessment of the importance of interception of private communications for the investigation, detection, prevention and prosecution of offences in Canada.

10.45 The Criminal Code provides in section 195.(4) that the Solicitor General of Canada shall cause a copy of each report prepared by him under subsection (1) to be laid before Parliament forthwith on completion thereof, or if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting. Furthermore, under subsection (5) the Attorney General of each province shall, as soon as possible after the end of each year, prepare and publish or otherwise make available to the public a report relating to-

(a) authorizations for which he and agents specially designated in writing by him for the purposes of section 185 made application, and

(b) authorizations given under section 188 for which peace officers specially designated by him for the purposes of that section made application,

and interceptions made thereunder in the immediately preceding year setting out, with such modifications as the circumstances require, the information described in subsections (2) and (3).

U. Written notification to be given

10.46 In terms of section 196. (1) of the Criminal Code the Attorney General of the province or the Solicitor General of Canada, as the case may, upon whose behalf authorization was sought and given for an interception, has to notify the object of an interception within ninety days after the period for which the authorization was given or renewed or within such other period as is fixed pursuant to the authorization. Notification has to be in writing, in a manner prescribed by regulations made by the Governor in Council, and it has to be certified to the court that gave the authorization that the person has been so notified. The running of the ninety days or of any other period fixed is suspended until any application made by the Attorney General or the Solicitor General to a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 for an extension or a subsequent extension of the period for which the authorization was given or renewed has been heard and disposed of.[34] Where the judge to whom such an application is made, on the basis of an affidavit submitted in support of the application, is satisfied that - (a) the investigation of the offence to which the authorization relates, or (b) a subsequent investigation of an offence listed in section 183 commenced as a result of information obtained from the investigation referred to in paragraph (a), is continuing and is of the opinion that the interests of justice warrant the granting of the application, the judge shall grant an extension, or a subsequent extension, of the period, each extension not to exceed three years.[35] The Criminal Code provides, finally, that an application pursuant to section 196.(2) shall be accompanied by an affidavit deposing to-

(a) the facts known or believed by the deponent and relied on to justify the belief that an extension should be granted; and

(b) the number of instances, if any, on which an application has, to the knowledge or belief of the deponent, been made under that subsection in relation to the particular authorization and on which the application was withdrawn or the application was not granted, the date on which each application was made and

---

34 Section 196.(2).

35 Section 196.(3).

the judge to whom each application was made.[36]

36 Section 196.(5) provides further that notwithstanding subsections (3) and 185(3), where the judge to whom an application referred to in subsection (2) or 185(2) is made, on the basis of an affidavit submitted in support of the application, is satisfied that the investigation is in relation to - (a) an offence under section 467.1, or (b) an offence committed for the benefit of, at the direction of or in association with a criminal organization, and is of the opinion that the interests of justice warrant the granting of the application, the judge shall grant an extension, or a subsequent extension, of the period, but no extension may exceed three years.

CHAPTER 11

COMMENTS AND RECOMMENDATIONS CONTAINED IN DISCUSSION PAPER 78

11.1 It was stated in discussion paper 78 that in general, the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), compares favourably with the legislation of the countries discussed above.

11.2 It was explained that the main difference is that, in South Africa, a specific judge or judges have been appointed to consider applications. In Belgium, France, the Netherlands and Germany, this power in respect of crime investigations is granted to a specific type of judge - the investigation judge - a concept unknown to our legal system. In France, the Netherlands and Germany this function is exercised by a political functionary in respect of security related investigation. It is, however, important that in terms of the South African legislation it is still a judge who has this power.

11.3 There is, therefore, in Germany, France, the Netherlands and the United States two systems - one for security monitoring and a system for criminal monitoring, with, in some instances, the control for the first on the Parliamentary level, and the control in respect of the second, on the judicial level. The South African law can be viewed in this sense to be more accountable than the European laws.

11.4 The new trend in Germany and the Netherlands, namely to place the burden of costs for creating the capability to monitor, on the Network Providers is interesting and should be noted. It may easily be that if the State assumes responsibility for these costs, that the State will keep on paying tremendous amounts only to keep track with technology, which is renewed every few months. The reality of the costs of cellular interception has hit those countries. In terms of the present wording of the South African Interception and Monitoring Prohibition Act, 1992, there is an obligation on the Network Providers to provide the necessary facilities and devices for the monitoring of conversations (an amendment in this regard to include all communications has already been approved by Parliament). The Government Departments, however, are responsible to pay for services in this regard, or at least the costs involved in providing those services.

11.5 The project committee made the following general recommendations in Discussion Paper 78, namely-

11.5.1 that the provisions in the Interception and Monitoring Prohibition Act, 1992 (section 5) be augmented by new provisions-

11.5.1.1 placing an obligation on service/network providers to ensure interceptability/monitoring of all communications;

11.5.1.2 setting out that the costs for enabling monitoring, ie providing the equipment and facilities shall lie with the Network/Service Provider and the personnel/administrative costs and recording of communications lie with the Government Departments involved, and a prohibition on the supply of communication services by the Network Providers which cannot be intercepted/monitored (the latter along the lines of the Netherlands' legislation).

11.6 The project committee made the following specific recommendations in regard to amending the Interception and Monitoring Prohibition Act, 1992, namely-

11.6.1 to insert a definition on call related information in order to define what call related information is, (however, the project committee posed the question whether its proposed definition is technically correct and considered that more attention should be given to the proposed definition and stated that it would appreciate receiving information particularly on this aspect);

11.6.2 to define further what a judge means in the context of the Act ie by substituting the term High Court for the term Supreme Court and to delete the reference to a particular division in regard to a retired judge who is designated by the Minister to perform the functions of a judge;

11.6.3 to make further provision in the definition of serious offence for offences to fall within the ambit of the Act ie to include other interests of the Republic (in addition to offences which may allegedly harm the economy and which are presently included as serious offences); any offence referred to in sections 13 (f) and 14 (b) of the Drugs and Drug Trafficking Act, 1992; any offence relating to the trafficking in firearms, ammunition and explosives; any offence relating

to the death or serious bodily harm of any person; and any offence relating to organized crime, money-laundering or the proceeds of crime. (The project committee noted that the definition of serious offence contains a proviso setting out that the offence concerned is being or has been committed over a lengthy period of time. The committee considered the question whether it is necessary to qualify the period over which an offence is planned or committed. One thought is that the lengthy period of time referred to in the definition sets the proviso in the scenario where the applicant must convince the judge of an ongoing offence to be monitored for a period of say 60 days. The committee also noted that the fact of the offence being linked to a lengthy period may present difficulties once the applicant has to satisfy the judge that the offence cannot be properly investigated in another less intrusive manner. The committee remarked that it did not, however, have definite views on the proviso regarding the requirement of the offence being committed over a lengthy period of time. The committee stated that it would appreciate receiving particular comment on this aspect.);

11.6.4 to insert into the definitions a definition on telecommunication service setting out that it means any telecommunication service as defined in the Telecommunications Act, 1996 (Act No. 103 of 1996), in respect of -

(a) a public switched telecommunication service;

(b) a mobile or a fixed cellular telecommunication service;

(c) a national long distance telecommunication service;

(d) an international telecommunication service; or

(e) any other telecommunication service licensed as such in terms of the Telecommunications Act, 1996. (The project committee also invited particular comment on the technical correctness of this proposed definition, since the question arises whether, for example, e-mail communication and video communications are included in its proposed definition.);

11.6.5 to make it further clear that the general position regarding interception or monitoring is that the interception or monitoring without the knowledge or permission of the parties to a conversation or communication so as to gather confidential information concerning any person body or organisation, is prohibited;

11.6.6 adding the interests of the Republic as another criterion to be taken into account by the judge when determining whether a direction should be issued to the existing criterion of the security of the Republic being threatened. (The project committee was of the view that its proposed term "interests" may lead to abuse if an application is brought on much narrower grounds than for example economic interests, and that more attention should therefore be given to the term "interests". The project committee therefore also requested specific comment on this issue.);

11.6.7 to provide that a direction may be issued by a judge designated by the Minister in each division to consider only applications in terms of the Act relating to serious offences; Provided that the Minister may designate a judge for more than one division; (Presently a direction may only be considered by the judge designated for the division from where the postal article or communication has been or will probably be dispatched or transmitted or where that postal article or communication will probably be received. However, presently only one judge has been designated for all the divisions who has to deal with all applications and no distinction is made between serious crime and security matters. Suggestions have in the past been made in Parliament to establish a panel of judges who should consider applications for interception and monitoring. In most of the European countries, there is a dual system in respect of security related/national interest investigations respectively and normal criminal investigations. It was suggested that a dual system also be created in the Interception and Monitoring Act in terms of which the National Intelligence Agency (NIA), the South African Secret Service (SASS) and the South African National Defence Force (SANDF) apply to a single judge at a central point for directions in regard to security and national interest matters, and that the South African Police Services (SAPS) also apply to the same judge for matters regarding national security. A further judge in each provincial and local division of the High Court could then be designated to consider applications for interception and monitoring in respect of the ordinary criminal investigations. However, a proviso was suggested empowering the Minister of Justice to designate a judge for more than one division dealing with the serious crime applications. The project committee favoured the appointment of a panel of judges.);

11.6.8 to substitute the term "convinced" in section 3(1)(b) of the Act with the term "satisfied". (The Act provides that a judge may issue a directive if the judge concerned is convinced that the offence that has been or is being committed or will probably be committed, is a serious offence that cannot be properly investigated in any other manner or that the security of the Republic is being threatened or that the gathering of information concerning a threat to the security of the Republic is necessary. The project committee considered that the required standard should be that of the judge being "satisfied" and not being "convinced". The project committee was of the view that the standard of being "satisfied" will be interpreted as meaning being satisfied on a balance of probabilities.);

11.6.9 to substitute the words "any other manner" with "another less intrusive manner" thereby making it clear that the offence concerned cannot be properly investigated in another less intrusive manner;

11.6.10 to provide in clause 3(7) that no communication between a legal representative and his or her client may be intercepted or monitored, except if on reliable information, the judge is satisfied that such a legal representative is involved in, or aiding or abetting a serious offence;

11.6.11 to provide in section 5(4) that the remuneration referred to in subsections (2) and (3) shall only be in respect of direct costs incurred in respect of personnel and administration and the lease of telecommunications lines, where applicable, and shall not include the costs of acquiring the facilities and devices referred to section 5A(2). (The project committee was however of the view that there is a need to give more attention to its proposed term "direct costs" with a view to establish whether "direct costs" is the appropriate term and also to establish what is exactly involved in "direct costs" and, further, it would like to ascertain what the amounts concerned are. The Act presently provides that if a person, body or organization has made a facility, device or telecommunications line available, for the purposes of the Act, the remuneration agreed upon by the person or organisation and the Commissioner of the South African Police Services, the Chief of the South African Defence Force or the Director-general of the Agency or Service, as the case may be, shall be paid to that person, body or organisation for assisting to execute a direction. If no agreement can be reached, a reasonable remuneration must be determined by the Minister for

Posts, Telecommunications and Broadcasting with the concurrence of the Minister for State Expenditure in order to compensate the person, body or organisation at least for any costs incurred as a result of any action taken in terms of the Act.);

11.6.12 to provide that no person, body or organization rendering a telecommunication service, may provide any such service which is not capable of being monitored;

11.6.13 to provide that any person, body or organization rendering a telecommunication service shall at own cost and within the period specified in a directive by the Minister responsible for Communications, acquire the necessary facilities and devices to enable the monitoring of conversations and communications, where the monitoring has been authorized in terms of this Act, from a supplier approved by the Minister responsible for Communications;

11.6.14 to provide that the investment, technical, maintenance and operating costs in making a telecommunication service capable of being monitored, shall be carried by the person, body or organization rendering such a service;

11.6.15 to provide that duplicate signals of conversations and communications authorized to be monitored in terms of this Act, shall be routed by the relevant person, body or organization rendering a telecommunication service to the relevant central monitoring centre, to be designated by, respectively, the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force, and the Directors-General of the Agency and Service;

11.6.16 to provide that the South African Police Service, the South African National Defence Force, the Agency and the Service shall, at State expense, equip and maintain central monitoring centres for the authorized monitoring of conversations or communications: Provided that an agreement on the sharing of any such central monitoring centre shall not be excluded;

11.6.17 to provide in section 5A(6) that the Minister responsible for Communications may issue a directive to any person, body or organization rendering a telecommunication service, to comply with the provisioning on the rendering of services which are capable of being monitored and that he or she may specify the security, technical and functional requirements of the facilities and devices to be acquired in terms of subsection (2);

11.6.18 to provide that any person who is authorized to apply for a monitoring or an

interception direction for the provisioning on an ongoing basis of call related data relating to the conversations or communications mentioned in the direction, and the judge may authorize such provisioning in the same direction;

11.6.19 to provide that any person, body or organization rendering a telecommunication service shall, in respect of all conversations or communications which are monitored in terms of this Act, route the call related data specified in a direction to the relevant designated central monitoring centre;

11.6.20 to provide that, if only call related data is required on an ongoing basis without the actual monitoring of the conversation or communication in question, the judge may direct that the relevant person, body or organization rendering a telecommunication service to whom or which a direction is addressed, provide such call related data for purposes relating to the functions of the South African Police Service, the South African National Defence Force, the Agency or the Service;

11.6.21 to provide that the procedures set out in the Bill in respect of the ongoing provisioning of call related data does not exclude the use of any other power in any other Act, to obtain evidence or information in respect of a person, body or organization;

11.6.22 to provide that any person, body or organization rendering a telecommunication service, shall provide such information regarding users of such telecommunication service to the South African Police Service, the South African National Defence Force, the Agency or the Service, as may be required by an officer or member referred to in sections 3(2)(a), (b) and (c) of the Act to fulfil the functions and exercise the powers authorized by law, including the provision of the name, identity number and address of the person using a specific telecommunication number;

11.6.23 to provide that any person, body or organization rendering a telecommunication service shall ensure that proper records regarding identities and addresses are kept in respect of clients to whom a telecommunication service is provided, whether on a prepaid or contract basis and shall require positive identification from a client to whom such a service is provided. (The project committee considered the term "positive identification" as a warning to persons, bodies or organizations rendering telecommunications services to be careful in their dealings with people particularly when confirming identification.);

11.6.24 to provide that a judge considering an application may dispense with the procedure set out in the Act in any case considered by him or her to be sufficiently urgent, and therefore he or she may deal with the matter in such manner and subject to such conditions as he or she may deem fit, including the grant in any appropriate case of an oral direction followed up by written application within one week. (This provision was introduced to deal with urgent or emergency applications. In Germany, the United States and some other countries the Attorney-General has such a power to grant authorization for interception and monitoring for a limited time, for example 24 hours. However, the Act does not presently make provision for the grant of directions in urgent circumstances enabling the judge considering the application to deviate from the procedure as set out in the Act.) The project committee was of the view that further attention should be given to the question whether the circumstances should be set out in the Bill in regard to urgent applications such as along the lines of the United States and Canadian legislation;

11.6.25 to set out that the use of any information obtained through the application of the Act, or any similar Act in another country, as evidence in any prosecution, is subject to any guide-lines of the Director of Public Prosecutions or Investigating Director concerned which may include an obligation to obtain the relevant Director's permission to use the said information as evidence, if so required by the Director of Public Prosecutions or Investigating Director. (Hence, the Act seeks to provide that evidence obtained from monitoring may only be used in a criminal trial with the authorization of the Director of Public Prosecutions or Investigating Director or person designated by him or her. The project committee considered that it is possible that there may be a number of cases being investigated in regard to a person being the subject of a monitoring and other cases might very well be put at risk if information or evidence uncovered by monitoring were to be disclosed if a Director of Public Prosecutions were not involved in the decision to use the information as evidence.);

11.6.26 setting out that the information regarding the commission of any criminal offence, obtained by means of any interception or monitoring in terms of the Act, or any similar Act in another country may be admissible as evidence in criminal proceedings. (The project committee was of the view that the question whether evidence should be admissible should be left to the trial court. The project

committee further noted the issue question whether evidence should be admissible in criminal proceedings irrespective of the grounds on which the direction has been granted, ie whether evidence obtained through monitoring should be admissible in respect of any criminal charge, irrespective of the grounds on which or the offence in respect of which the authorization was obtained. The project committee noted section 35(5) of the Constitution which provides that evidence obtained in a manner that violates any right in the Bill must be excluded if the admission of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice. The committee noted further that a pertinent question is whether it would be thought unconstitutional to allow evidence obtained as a result of a lawful direction which was authorised in respect of an offence other than the offence uncovered by the monitoring. The project committee was of the view that the application of this clause should be confined to serious offences only. The project committee considered that there are two options in regard of the proposed clause: The first option was to retain the wording of the proposed clause which means that all evidence uncovered by a monitoring may be presented and the court then has to decide whether the evidence is admissible. The second option was to delete the words "irrespective of the grounds on which the direction has been granted".)

11.6.27 to provide that any person, body or organization rendering a telecommunication service and who or which fails or refuses to comply with -

(a) a direction issued by a judge;

(b) a directive issued by the Minister for Posts, Telecommunications and Broadcasting;

(c) the obligation to provide information regarding a user of a telecommunication service; or

(d) the obligation to keep records; or

(e) the obligation to require positive identification when contracting a telecommunication service;

shall be guilty of an offence, and liable on conviction, to a fine.

(The project committee noted that section 8(1) of the Act does not prescribe a maximum fine which may be imposed if a party contravenes the provision. The project committee was of the view that further attention should be given to this aspect and that a substantial amount should be set in regard to the proposed

clause 8A(1) of the bill and section 8(1) of the Act. The Committee was of the view that R 200 000-00 is an appropriate maximum amount to be considered in respect of the proposed clause 8(1A) of the Bill in view of the seriousness of the issues concerned. The project committee noted that the Australian Federal Telecommunications (Interception) Act provides that the penalty for authorizing, suffering or permitting another person to intercept or to do anything that will enable a person to intercept a communication is $ 5 000-00 or imprisonment for 2 years. The project committee therefore considered that the maximum fine in regard to section 8(1)(a) should be R 20 000-00 and in regard to section 8(1)(b) an amount of R 40 000-00 .)

11.6.28 to provide that if any person, body or organization who or which renders a telecommunication service, after a conviction for failing to comply with a directive, fails to comply with a further directive issued by the Minister for Posts, Telecommunications and Broadcasting to comply, the Minister may revoke the licence issued in terms of Chapter V of the Telecommunications Act, 1996, to such person, body or organization to render a telecommunication service.

11.7 The project committee further requested particular comment on the following issues:

11.7.1 Regulating the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices:

The project committee considered that a matter which is alarming in South Africa, is the large number of advertisements, sometimes even in law journals of private investigators, offering to deliver services which include "bugging". Furthermore, the project committee was of the opinion that in view of the fact that only the South African Police Service, the South African Secret Service, the South African National Defence Force and the National Intelligence Agency may be authorized to do interception and monitoring, the legality of monitoring in certain circumstances by private investigators is questionable, especially in regard to instances of third party monitoring. The project committee also noted that in the United States of America the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices is prohibited, and that such a device s defined as one which "renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications". The Committee noted that

it is accepted that video and recording equipment may be misused for the purpose of illegal and " surreptitious" monitoring and that the policing of such a prohibition might be problematic. Moreover, the committee noted that the Hong Kong Law Reform Commission held the view that in view of the apparent lack of effectiveness of existing controls on the availability of surveillance equipment, they were unable to recommend the enactment of any additional legislative controls on this matter.

11.7.2 The project committee requested comment particularly on the question of whether respondents are of the view that the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices should be regulated, and if so, which measures should be adopted.

11.8 Third party surveillance:

11.8.1 The project committee considered that the Interception and Monitoring Prohibition Act, 1992, should also be amended by clearly stating that only third party surveillance is included in the prohibition. (It was considered that a police agent recording his own conversation with the leader of an infiltrated syndicate should, therefore, not be affected by the prohibition.) The project committee considered that this is already implied by the present Act, but that it should be re-formulated to make it more clear.

11.9 Should the Act be more prescriptive?

11.9.1 The project committee noted that the Hong Kong and Canadian legislation is very prescriptive in regard to the procedures to be complied with. The committee requested particular comment on the question of whether the Bill should set out the procedures to be followed under the Act in more detail.

It was pointed out that the Minister of Justice is responsible for the administration of the Interception and Monitoring Prohibition Act, 1992.

A draft Bill, in which the above provisional proposals were addressed in Discussion paper 78, is attached as Annexure "C".

CHAPTER 12

COMMENTS RECEIVED ON DISCUSSION PAPER 78, EVALUATION AND RECOMMENDATIONS

12.1 Introduction

12.1.1 A number of respondents made general remarks besides commenting on particular aspects of the proposed Bill. The Department of Welfare comments in general terms by saying that it supports the Commission's efforts to reinforce measures such as the Bill designed to fight organised crime in South Africa. Telkom notes that the proposed Bill seeks to place an obligation on telecommunication networks and service providers of ensuring the interceptability and capacity to be monitored of all communications, a prohibition on the supply of communication services by telecommunication network/service providers which cannot be intercepted or monitored, and the obligation and cost of providing the equipment and facilities used to intercept and monitor communications on network/service providers as opposed to placing it on the respective government departments concerned.

12.1.2 Telkom states that its concern is that although this proposition may seem to be an elegant and cost effective solution to the problem faced by government of ensuring that it can effectively intercept and monitor communications in an environment of rapid and sometimes bewildering technological change in telecommunications, the proposals give rise to a plethora of problems, some of which may be considered intractable, or at the very least would require a reconsideration of the premise on which the new approach to interception and monitoring is based. Telkom considers that the requirement that the telecommunication network/service provider must ensure the interceptability /monitoring of communications raises a number of issues which are not addressed in the discussion paper.

12.1.3 Telkom considers that, to begin with, South Africa has a considerable amount of built network telecommunications capacity which cannot, except at prohibitive cost, be rendered capable of being intercepted or monitored at will. Telkom notes that the financial implications of ensuring the interceptability/monitoring of communications, particularly in a context where there are no stipulations as to the cost, affordability, grade of service and the reasonableness of requirements, would undermine the telecommunications policy framework

which the government has so assiduously crafted. Telkom considers that there will clearly be a trade-off between its mandate to renew and extend the existing telecommunications network with limited resources and under considerable time pressure, particularly to under-served and previously disadvantaged communities, and meeting new and rather onerous obligations on interception and monitoring to the detriment of the former.

12.1.4 Telkom notes that there is also little or no clarity as to what the extent of Telkom's responsibilities are, as both a network and service provider, particularly with respect to service providers reliant on Telkom's network. A general obligation is placed on network/service providers described in the Draft Bill as telecommunications service providers '... to acquire the necessary facilities and devices to enable the monitoring of conversations and communications..." The Telecommunications Act 103 of 1996 provides that a Private Telecommunications Networks (PTN's), other than those of a few defined parties, shall not be provided by means of telecommunications facilities other than facilities made available by Telkom. In turn Value Added Networks Services (VANS) shall only be provided by means of facilities made available by Telkom. Telkom considers that in the light of the explicit provisions of the Telecommunications Act determining the responsibility of either Telkom or the service provider for interception and monitoring becomes an increasingly complex task.

12.1.5 Telkom states that the question to be answered in this instance is whether Telkom, as both a network and service provider, is responsible for the interception and monitoring of VANS services that it provides. If so, what is the nature and extent of the interception and monitoring service to be provided by a Telkom VAN which makes use of the Telkom network infrastructure. Would a Telkom VAN be responsible for the decryption of encoded data on its networks or merely for an interception and monitoring service? If it is not responsible for decryption, is the responsibility for interception and monitoring correctly placed and should it not be the sole responsibility of the network provider to intercept and monitor communications on its own network. It should however be noted that the capacity of a network provider to do so may also be limited by how effectively it can deal with the problems posed by the various network architectures and encryption of these networks.

12.1.6 Telkom considers that with respect to PTNS, which encompass both national and international telecommunication networks and carry the traffic of a single party, usually that of a corporate person, a number of questions arise from the proposals contained in the Draft Bill.

Principally the question to be answered is should a PTN intercept and monitor its own communications and thus become a party to interception and monitoring or is the network provider to be tasked with the end to end responsibility for interception and monitoring of networks, whose scale, complexity and international reach would require the cooperation of not only other international network providers but also the administrative authorities of third countries, all at prohibitive cost. Telkom remarks that again where the responsibility lies for the decryption of communications on such networks is not clear.

12.1.7 Telkom notes that with respect to the VANS of third parties which make use of Telkom facilities the Draft Bill provides that as service providers they shall be responsible for interception and monitoring of communications on their networks. Of general concern to Telkom is whether they have capacity to do so at a cost that would not prove prohibitive and would destroy any competitive advantages they may have. Telkom states that it is also not clear if the point of intervention with respect to VANS has been correctly identified. By law VANS must make use of the telecommunication facilities of network providers. Making VANS responsible for interception, monitoring and by implication decryption of communications, may result in undue interference and degradation of the telecommunication facilities of the network providers, particularly in the context where the responsibility for the provision of interception and monitoring as between network service providers and VANS is not clearly ascertainable. Telkom considers that the temptation on the part of VANS to carry out statutory obligations at least cost where there is no countervailing obligation to assure the integrity of the network would be high.

12.1.8 Telkom suggests that from the foregoing, it is believed that the roles, responsibilities, functional capabilities and capacities of the various actors in the telecommunications industry need to be re-examined and re - defined as well as the nature of the interaction between the various parties.

12.1.9 The Mobile Telephone Networks (Pty) Limited (MTN) states that whilst it recognises its responsibility of assisting the Security Structures in South Africa in maintaining safety and security, it also has a responsibility to its customers to protect the constitutional right to privacy. MTN will not comment in detail on each and every recommendation made by the Commission. Due to the limited time granted to make comments on this particular project, MTN does also not in detail make comments on any legislation in other jurisdictions.

12.1.10 MTN agrees that electronic surveillance does play an indispensable role in the detection of sophisticated criminal enterprises. However, it is necessary to strike a reasonable balance between the right to privacy as enumerated in the Constitution of the Republic of South Africa and the right of the State to intrude on privacy in the furtherance of its responsibilities for law enforcement. According to statistics released by the administrative office of the US Courts and the Department of Justice in the USA, court orders for electronic surveillance by state and federal agencies for criminal purposes as well as criminal and national security investigations increased substantially in 1996. MTN notes that in all, interceptions were in effect for a total of 43 635 days in 1996. Moreover, according to the report, electronic surveillance continues to be relatively inefficient. Overall, 2.2 million conversations were captured in 1996. A total of 1.7 million intercepted conversations were deemed not "incriminating" by Prosecutors. Each interception resulted in a capture of an average of 1 969 conversations. Of these conversations Prosecutors reported that on average 21.4% were "incriminating".

12.1.11 MNT considers that a society which exposes its citizens, at the whim of the State, to the risk of having a permanent electronic recording of its citizens' words made everytime they open their mouths may be superbly equipped to fight crime but would be one in which privacy no longer has any meaning. MTN is therefore of the view that any legislative scheme should set a high standard for obtaining these authorisations.

12.1.12 MTN considers that it follows then that an external and objective criteria should be set to afford a measure of protection to any citizen whose private communications have been or are going to be intercepted. It should then become possible for the individual to call the State into account if they can establish if a given interception was not authorised in accordance with the requisite standard. MTN notes that the need to protect individual privacy from government intrusion becomes ever more critical as the means and opportunities to invade privacy increase. Clear rules and guidelines protecting the privacy of communication and limiting the government's ability to intercept electronic communications surreptitiously need to be advanced and agreed upon.

12.1.13 MTN considers that the South African's public privacy must be protected to the greatest extent possible while, at the same time, providing for legitimate law enforcement needs. It should reflect the unambiguous commitment of the Government of the Republic that compliance with law enforcement needs should not interfere with the tremendous benefits

provided by telecommunications technology and services, as indeed envisaged in the telecommunications White Paper published by the Department of Communications. MTN suggests that in part this is because electronic surveillance poses greater threats to privacy than do physical searches and seizures and that electronic surveillance tends to be indiscriminate, catching communications that may not even be relevant to an investigation much less contemplated by a Court Order. Electronic surveillance also tends to extend for long stretches of time. Moreover, it is conducted surreptitiously and without notice to the subject and other persons participating in electronic communications.

12.1.14 MTN states that on the question of obtaining the exact location of a subject or subject being tracked it must be mentioned that law enforcement has been undertaken without telephone location tracking information for centuries. It is therefore clear that law enforcement in utilising such technologies would, in fact, expand the government's ability to conduct electronic surveillance while making traditional methods of surveillance unnecessary. Because of the mobility involved in wireless communications, the physical location of a caller may reveal sensitive or confidential information concerning the caller's travel. MTN remarks that for instance, a cellular caller may be using his telephone in his Attorney's office while conducting privileged business. MTN considers that if law enforcement officers wish to track someone they can use traditional surveillance methods and stakeouts to follow a person's progress through public areas. MTN remarks that it is very surprising and in their view unacceptable that a network operator could be burdened to supply and develop tracking systems so that in effect such network operator would become a police agent and additionally, not be able to be reimbursed for the costs except direct costs as envisaged in the current proposal in the Bill.

12.1.15 MTN states that it should be further be noted that in the US the Statute relating to "tapping" specifically stated that carriers or network operators could be required to modify their systems for law enforcement purposes only if the changes were "reasonably achievable". MTN considers that the proposed amendments and proposals made by the Commission bring to the fore the intent of the drafters of the Bill that each and every obligation placed on the State in terms of the current Monitoring Act, be diluted. As examples of this trend in the proposals, MTN cites the fact that the Judge concerned need not be "convinced" of the facts before him but only be "satisfied". MTN further notes that despite the fact that the current Monitoring Act adequately provides for information to be gathered in such a intrusive manner, the proposals currently suggested seem to want to make an intrusive method of gathering information, more

intrusive to the extent that it may not be reasonable.

12.1.16 MTN notes that the *Naidoo* case quoted in Chapter 1 of the report states that "what is clear is, probably after the experience of police methods during the apartheid era, the legislature saw fit to repeal the old provisions relating to interception of personal articles, telephone communications, etc in terms of which various Ministers could authorise such actions and to replace those provisions with the obviously extremely stringent and limited provisions of the Monitoring Act". MTN remarks that quite clearly the judge in this matter made commentary by implication on the unacceptable police methods used during the apartheid era. MTN is of the view that should the proposed Bill be accepted in its current format, the abovementioned quoted comments would be apposite. MTN further questions whether the proposals contained in the Bill would not fall foul of section 36 of the Constitution. MTN notes that the Constitution states that a law of general application "will only find application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom ...". MTN is of the opinion that on the whole, the proposals contained in the Bill are grossly unreasonable, not only towards Service Providers or Network Operators but also to the general public.

12.1.17 MTN notes that it relies heavily on the South African Telecommunications Regulatory Authority ("SATRA") to investigate any matters of frequency interference and it needs to be questioned how this particular Act and proposals affect the monitoring and enforcement practices as currently rendered by SATRA. MTN remarks that should this Act prohibit SATRA from doing its normal monitoring on complaints received of frequency interference, then any Network Operator utilising frequency spectrum in South Africa will be put at a disadvantage and indeed prejudiced. MTN states that every interference problem investigated by SATRA is done by monitoring and the use of direction finding equipment.

12.1.18 MTN considers that the Monitoring Act should be intended to balance three key policies:

- to preserve a narrowly focussed capability for law enforcement agencies to carry out properly authorised intercepts;
- to protect privacy in the face of increasingly powerful and personally revealing technology; and

- to avoid impeding the development of new communication services and technologies.

12.1.19 MTN considers that to maintain a balance, detailed guidelines should be established on how industries standard setting organisations would accomplish the costly mandate of the Monitoring Act and should impose several obligations on law enforcement to facilitate the process as well. MTN states that the Monitoring Act should also provide that an industry association or a standards-setting organisation will set the technical standards; the Attorney General or Minister of Justice must consult with the standard-setting organisations with representatives of users of telecommunications equipment, facilities and services, and with SATRA, to ensure the efficient and industry-wide implementation of the requirements envisaged in the Bill. MTN considers that this requirement has clearly not been included in the Bill.

12.1.20 MTN remarks that it further seems that in terms of checks and balances required, this Act should require the Attorney General or Minister of Justice to provide a numerical estimate of law enforcement's anticipated use of electronic surveillance for 1999 and the future. MTN considers that by mandating this publication of numerical estimates of law enforcement surveillance activity, it will serve as mechanisms that will allow Governmental and public oversights. MTN suggests that the purpose behind such provision is to ensure that Network Operators receive adequate and specific notice from the Attorney General or Minister of Justice about the needs of law enforcement.

12.1.21 MTN considers that it should be stated policy that law enforcement agencies be denied the authority to dictate the design of telecommunications networks under this Monitoring Act by conferring this authority to telecommunications industry associations where all parties with an interest would be able to have input.

12.1.22 The South African Telecommunications Regulatory Authority (SATRA) notes that the Interception and Monitoring Prohibition Act No 127 of 1992 has withstood the scrutiny of the South African courts. SATRA remarks that the principle that the right to privacy is not absolute has been established in our case law. SATRA's primary concern in considering the proposed amendments to the Act has been that the amendments will also withstand the inevitable Constitutional challenges that will be made once the amendments are promulgated. In addition, SATRA has, as a regulatory authority, considered the feasibility, desirability and enforceability

of the proposed amendments. As a licencing authority, SATRA has evaluated the proposed amendments in the light of the additional obligations it anticipates it will attract if the amendments are passed into law.

12.1.23 M-Web states that in principle they remain unconvinced that the Discussion Paper provides sufficient evidence to justify the proposed amendments and that at the very best the Act should only be amended to clarify the definition of communications which may be intercepted or monitored. M-Web considers that the burden should remain on the State to have the necessary facilities and devices in place which it may require to intercept and monitor defined communications as may be authorised from time to time and that the general tenor of the legislation should be drafted accordingly. M-Web remarks that they acknowledge that organized crime may require a review of existing legislation. However, the Discussion Paper reveals no evidence of the extent to which modern communications technology has increased the levels of such crime or assists in the perpetration of such crime in South Africa. M-Web considers that in the absence of such evidence the proposed amendments to the Act may not pass constitutional muster as there may be no rational basis for the imposition of potentially overbroad obligations on a telecommunications services licensee.

12.1.24 Reuters remarks that it operates at the hub of one of the world's largest global private networks, and relies on many telecommunications providers in order to build secure, high-value information and electronic trading services. Reuters also offers certain services, such as electronic mail, which may (now or in the future) fall within the scope of the proposed South African legislation. But whatever the style of service, financial organisations in South Africa and globally rely on the accuracy and freedom from bias of Reuters information. Reuters remarks that that their business depends on their customers' ongoing trust in the security and integrity of their communications.

12.1.25 Reuters considers that despite the claimed law enforcement benefits of installing monitoring equipment for telecommunications services, there are two major drawbacks to the proposals. First, the cost and complexity that would have to be borne by the service providers. Second, the impact that such monitoring facilities would have on the ability of businesses to build robust, trustworthy, commercially attractive, on-line services. Reuters state that there may also be issues of individual privacy, but they will not address these further here. Reuters state that at present the cost and technical complexity, or even feasibility, of installing and operating

the monitoring facilities are unknown. Reuters consider that this would be a disincentive for telecommunications operators who might otherwise seek to expand in South Africa. Reuters ask that these issues be quantified, and weighed against the likely number of successful intercepts, before any commitment to legislation is made. Reuters states that in the meantime it is opposed to this new burden being placed on service providers.

12.1.26 Reuters remark that trust is a vital concept for electronic commerce, and other business services offered over telecommunications services. Reuters state that the participants in electronic business have certain expectations of security, in particular, that their information will remain private and under their control. This is particularly the case in the banking sector, which influences many of Reuters' most important customers. Reuters imports huge amounts of confidential data owned by banks over its networks. Reuters note that if the underlying technical infrastructure is not trusted by the customers, then profitable, high-value services cannot operate. The impact of monitoring would therefore be to damage the potential for South Africa based companies to participate fully in the growth of global electronic commerce.

12.1.27 Mr Harold Marshall[1] remarks that it is essential that the privacy of the individual is maintained. Careful consideration must be given and the guidelines for investigating officers must be very clear. Consideration must also be given to the rights of an individual or company to be able to protect their assets against criminal activities. He states that the legal occupier of any premises has the right to privacy at these premises as well as the right to protect their assets, against any illegal activities. Mr Marshall points out that the telecommunication system within the company belongs to the company concerned and that all equipment used by the company and on the premises are the property of the company. He also suggests that all this equipment is used by a company or organisation for the purpose of carrying out its objectives. He considers that the use of facilities are provided by the company for company purposes and for the benefit of the company and the use of these facilities by any person for private purposes remains at the discretion of the company.

12.1.28 Mr Marshall suggests that if a company has reason to believe that there is any illegal activity, which will be detrimental to the company, the company must have the right to

---

1 Of Marshall International Sales whose products and services include electronic security, counter espionage equipment, surveillance systems, audio and video recording equipment, cctv equipment, telephone monitoring equipment, radio communications.

carry out, on their property, any surveillance or interception or monitoring of their equipment or premises and this should not be considered illegal or un-authorised. He proposes that evidence obtained in this way should be admissible in court and authorisation by a Judge should not be required in this case. He notes that if a Law Enforcement Agency or a private investigation agency is called in, they will automatically have the permission of the owner of the company to monitor on the premises and that by registering a case with the Police should be sufficient authorisation for a private investigator or the company security officer to continue monitoring and surveillance. Mr Marshall considers that if it becomes necessary to monitor the private property of an individual without the consent of the occupier, then the Police must make the application to a Judge. He suggests that the owner of the Company does not have the right to carry out monitoring of an employees residence and must revert the case to the Police. He remarks that the Police should also be able to authorise a private investigator to carry out surveillance, interception and monitoring and to assist with an application to the Judge, and the company owner can monitor any activity in a public place, eg monitoring his own vehicles or staff activity whilst in the performance of their duties.

12.2.1.29 Mr Marshall points out that, at this moment, the SA Police Services are inundated with work and that it is therefore understandable that they cannot investigate a crime until positive proof has been given to them. He notes that it is for this reason that large companies employ their own security staff or use private investigators for investigations, and that these investigators will then obtain sufficient evidence to be able to open a docket and the police can proceed further. Mr Marshall notes, however, that confidentiality is important and that confidentiality between the complainant and the Police must remain confidential. He suggests that this information should not become available to any one not directly connected with the investigation. He considers that the law must also allow the exchange of information between different Law Enforcement Agencies and that during the course of an investigation, information may come to light about other criminal activities which fall under a different department. He suggests that provision should be made within the Act to allow for this exchange.

12.1.30 The SAPS[2] notes that according to a newspaper report[3] telecommunication

---

2 Chief Manager Legal Component Detective Services.

3 Beeld 1998-12-15.

service providers welcomed the proposed amendments to the Interception and Monitoring Prohibition Act, 1992, but warned that it is *"unpractical"*. The SAPS notes that MTN and Vodacom, according to the report indicated that they will comply with the prescribed requirements, if it is fair and respects the privacy of their clients. They state that Mr Jacques Selschop of MTN is quoted that it is almost impossible to exercise control over the particulars or persons who make use of prepaid packages. They note that he also said that it is practically impossible intercept a call between two cellphones:

> "Oproepe tussen twee selfone kan net by 'n oorskakelpunt onderskep word. MTN is nie bewus van die bestaan van toerusting wat dit kan doen nie en as daar is, sal dit miljoene rande per eenheid kos. Die toerusting sal by elkeen van sy oorskakelpunte geïnstalleer moet word.-"

12.1.31 The SAPS states that it does not wish to enter into a public debate with MTN on the matter, either regarding the costs or the technical capabilities. They consider that to publicly announce all technical capabilities of equipment which is available, will be detrimental to law enforcement, as well. The SAPS proposes that a recommendation in this regard would be incomplete without a briefing on the technical aspects. The SAPS proposes to arrange a confidential briefing by the intelligence community to the Project Committee in this regard. At this briefing the committee could also be informed of the experience of police services in Europe relating to interception and monitoring which experience they have shared with the SAPS. The SAPS remarks that the draft Bill reflects in their opinion correctly on how present technology could be utilized to monitor all types of communications.

12.2 SPECIFIC COMMENTS ON THE BILL

12.2.1 Clause 1(a): definition of call related information

(a) The definition proposed in the Bill

12.2.1.1 The definition contained in the Bill suggested by the project committee was drafted as follows:

> "Call related information includes dialling or signalling information that identifies the origin, direction, destination, termination, duration and equipment identification of each

communication generated or received by a user of any equipment, facility or service of a person, body or organization rendering a telecommunication service and where applicable the location of such user.

(b) Comments on the proposed definition

12.2.1.2 Adv Mnyatheli of the Investigative Directorate Serious Economic Offences notes that this refers to what is known as call line identification (CLI) in telecommunication terms. It normally enables the identification of the caller both in fixed and in cellular telephones, the position of location of a call. This is obviously very useful data for telecommunication users. Adv Mnyatheli remarks that as the definition correctly indicates, it also informs as to where the call is made, and again this can help a lot with regard to detection of crime. He is, however, not so certain as to whether technology now allows one to detect the type of equipment facility that the caller is using. He is aware that a lot of energy is now being spent on developing technology that will enable one to see the caller, but the equipment facility identification, is a matter which he considers would take some time to develop. Whilst this definition captures most possibilities, to the extent that it refers to equipment identification it may be inaccurate. Adv Mnyatheli would therefore suggest that reference to equipment identification be omitted. When certainty regarding the possibility of identification of equipment has been gained this definition may be re-visited and provision may accordingly. He suggests a more general approach as follows:

" Call-related information includes dialling or signalling information that identifies the origin, direction, destination termination, duration and any other information connected with that call or communication generated or received by a user of any equipment, facility or service of a person, body or organization rendering a telecommunication service, and where applicable the location of such user".

12.2.1.3 Adv Mnyatheli explains that he makes this suggestion not only because the Telecommunications Act does not define *call-related information,* but also because technologies change from time to time, and therefore, from a legal point of view it is inadvisable to have a restrictive definition in a field that does not belong with law. A possibility also exists that what may be regarded as call-related information by one telecommunications operator may not be such to another telecommunications operator depending on the type of equipment they may be using and the purpose therefor. The above definition therefore also stands to vary from time to time.

12.2.1.4 MTN is of the view that the extent of the information required is too great. MTN states that the question needs to be asked as to why signalling information that identifies *inter alia* the origin and direction is needed by the Police and other Security Structures. MTN asks whether it is envisaged that the Network Operator divulge sensitive transmission link related information or routing information to comply with this requirement? If this is the intention MTN is of the view that it places a prejudicial burden on MTN due to the nature and frequency of changes made in the infrastructure of a Network Operator for optimum performance.

12.2.1.5 MTN notes that the proposed definition also mentions the fact that information relating to the location of such user be included in call-related information. MTN considers that the intention of the proposal is very clear in that it would be required of the Service Provider or Network Operator to become an Agency of the Police or Security Structures in that such Network Operator would be obliged to become the follower or "agtervolger" of the target. MTN notes that it seems grossly unreasonable that the State would, it seems, without cost to itself, oblige a Network Operator to "follow" the target.

12.2.1.6 MTN states that the extent of the current proposed definition would allow for all information relating to each and every call identified by the Judge's directive be sent through to the Police or Security Structures concerned. MTN considers that the administrative, technical and financial load placed upon the Network Operator would be of such an extent, to be deemed unreasonable.

12.2.1.7 The National Intelligence Agency states that one institution may be the network provider to enable another institution to provide a service to a customer through a lease agreement. The NIA notes that some call-related data will be with the one and other with the other institution, and asks whether both will be regarded as a "person, body or organization rendering a telecommunications service"? The NIA also remarks that they would like the Commission to consider whether the present definition of "telecommunications line" in section 1 of the Act is wide enough to provide for the interception of modern-day communications such as "e-mail'.

12.2.1.8 The following comments were made in a submission received from the Director

of Public Prosecutions of the Cape of Good Hope[4]:

> Daar word aanbeveel dat 'call-related information' nie in hierdie wet opgeneem word nie en wel om die volgende redes: 'Call-related information" word gesien as onder andere omvattende die volgende inligting:
>
> (a) Die telefoonnommer;
> (b) Die gedetailleerde inligting van die betrokke telefoonoproepe gernaak detailed billing);
> (c) Die plek van waar die telefoonoproep gemeak word naamlik, die toring wat deur die selfoongebruiker benut word;
> (d) Die datum en tyd wat geskakel is;
> (e) Die tydsduur van die gesprek.
>
> Indien hierdie definisie in die wet geplaas word sal dit beteken dat enige persoon wat in die vroeë stadium van die ondersoek is, 'n aansoek sal moet bring ingevolge Wet 127 van 1992. Hierdie aansoeke is tydrowend en met die huidige posisie dat daar slegs een Regter aangewys is te Pretoria sal dit nie doeltreffend wees om hierdie tipe inligting deur middel van die onderhawige wet te bekom nie'.
>
> In die ondersoek van georganiseerde misdaad word inligting dikwels slegs vir verdere ondersoekdoeleindes benut en sal die betrokke ondersoekbeampte nie 'n aansoek ingevolge die onderhawige wet kan) regverdig nie en sal hy derhalwe nie geregtig wees om inligting ten opsigte van sogenaamde 'flagging' te bekom nie.
>
> Dit blyk dat ondersoekers in dwelm aangeleenthede nie van hierdia wet gebruik hoef te maak nie as gekyk word na die beoogte wysiging van sub-artikel 5B(4).
>
> Die vraag wat egter ontstaan is dat indien hierdie bepaling in die wet ingesluit word daar geargumenteer kan word dat daar slegs ingevolge Wet 127 van 1992 magtiging bekom word om die sogenaamde 'call-related information" te bekom. Die toepassing van Wet 127 van 1992 soos dit tans is lewer reeds groot probleme met toepassing in die praktyk en word daar aanbeveel dat daar met groot omsigtigheid gekyk word na welke aspekte in hierdie betrokke wet beliggaam moet word. Dit is die Respondent se aanbeveling dat die idee goed is dat die bekom van "call-related incidents" statutêr gereël word, maar daar word aanbeveel dat daar nie in hierdie betrokke wysigingswet daarmee gehandel word nie, maar dat daar eerder oorweging aan geskenk word om hierdie aspek te behandel in 'n strafproseswysigingswet.

12.2.1.9 Vodacom recommends that this Act be amended to refer only to "communications" in order to avoid "hair-splitting" legal disputes. Vodacom explains that for example, an SMS or e-mail is like a telegram (ie it is dispatched without the certainty of a reply, which a conversation would require). A call to a person's cellphone may result in a

---

4 And in a similarly drafted submission made by the Office of the Director Investigating Directorate Organised Crime and Public Safety.

conversation, but if the call is routed to voicemail, it will result in something more like a telegram. Vodacom states that it is questionable whether two computers "converse" in the course of a data communication and asks whether an Internet "chat" site is a place of "conversation"? Vodacom suggests furthermore, that the Commission needs to consider, comprehensively, the usefulness of the historic distinction between something physically "intercepted" - ie seized or stopped in its path and read and listened to - and then possibly returned into the stream of communication (eg a letter), versus something being rendered capable of monitoring by duplication or adding an additional "party" to the communication, eg a conference call.

12.2.1.10 Vodacom notes secondly, that the purpose of the Act is to provide for the monitoring and interception of conversations and communications. Vadacom therefore interprets the inclusion of the words "location of the user" in the definition of "call-related data" to mean *the location of the user at the time of the initiation or first reception of a call.* Vodacom considers that mobile network operators technically cannot, and in terms of this Act should not be required to provide data as to *the continuing movement* of a user during a call. Vodacom remarks that judges will have to carefully consider the level of intrusion (and necessity) of locational data when considering applications (i) for directives including call-related data in the context of full interception or monitoring, or (ii) for directives for call-related data only, particularly if it is to be provided on an ongoing basis or over a significant period of time. Finally, Vodacom states that it is not clear as to the meaning of the "direction" of a call. In June 1999 Vodacom submitted a further comment to the Commission. Vodacom considers that the purpose of the Act is to provide for the monitoring of conversations, communications and postal articles and not ongoing surveillance. Vodacom therefore proposes that the inclusion of the phrase "*location of the user*" in the definition should be interpreted to mean "location of the user at the time of the initiation or first reception of a call. They also consider that the words "*origin*" and "*destination*" makes the inclusion of the words "*direction of a call*" seem superfluous and suggest the following definition:

> "'call-related information' includes dialling or signalling information, that identifies the origin, destination, termination duration and equipment identification of each communication generated or received by a user of any equipment, facility or service of a person, body or organisation rendering a telecommunication service, and where applicable the location of such user at the time of the initiation or first reception of a call."

12.2.1.11 Telkom notes that the term 'user' is too generic, broad and not defined. Telkom

suggests that in a public network environment the term "customer" would be more specific and preferable. Telkom remarks further that it is not known what is meant by "equipment identification' and in the absence of clarity of the matter, the words should preferably be deleted. Telkom notes that the Judicial Matters Amendment Act,1998 introduces the concept of 'communication' which is not defined. Telkom considers that it is presumably meant to cover non-voice telecommunications. It would be preferable if it were defined. Telkom considers that a subsidiary problem is to be found in the definition of 'telecommunications line' which is almost, but not quite the aggregate of the definitions of "signal", "telecommunication" and "telecommunication facility" in the Telecommunications Act, 103 of 1996. Telkom considers that it would be preferable if the definitions provided in the Telecommunications Act were used.

12.2.1.12 Telkom points out that with respect to certain types of equipment, it should be noted that not all the call information can be provided. Telkom considers that the implications on a network provider, providing call-related information in respect of Value Added Network Services (VANS) and Private Telecommunication Networks (PTN's), who are service providers in their own right, but who use the network of the Network Service Provider, needs to be considered. Telkom proposes that the section be amended to read as follows:

> "call-related information" means, to the extent that is possible to provide such information **[includes]** dialling or signalling information, that identifies the origin, direction, destination termination, and duration and equipment identification of each communication generated or received by a customer leasing such service from **[user of any equipment, facility or service of]** a person, body or organisation rendering a telecommunication service, and where applicable the location of such customer **[user.]**'

12.2.1.13 The SAPS[5] remarks that service providers require section 205 subpoenas for call-related information (detail billing and ownership). The SAPS makes the suggestion that a direction should cover all relevant info regarding suspects without issuing a 205 subpoena. This will only apply on info gathered through a direction. The SAPS states that it happens on a regular basis that suspects and accomplices leave messages without names. For the Investigating Officer it is imperative to find out who the contact person was and to find out who accomplices are with regards to name and residential addresses. Sometimes the information is of critical importance especially in murder investigations, escaping from lawful custody as to ascertain where suspects are hiding - especially when they are on the move it is of utmost

---

5 Office of the Commander Technical Support Unit Eastern Cape.

importance to get info as soon as possible. It is also required to launch police actions with regard to drug-trafficking deals. They state that currently a 205 subpoena is required and because of that valuable time is wasted to apprehend suspects when still at a specific address, etc.

12.2.1.14 The SAPS[6] comments that it should firstly be stated that it is difficult to draft an exhaustive definition of call-related information. They state that the proposed definition is supported in view of the fact that it is not all inclusive, as indicated by the word *"includes"*. The SAPS considers that it may be improved by inserting the word "also" before "includes'.. In practice, it is accepted that an agency will apply for a direction in respect of call-related information and it could be accepted that the specific type of information requested, will be specified in the application, as well as the direction of the judge. The SAPS notes that in respect of the words "and where applicable in the proposed definition the *location of such user"* it should be reformulated in view of the fact that only the cell (in respect of mobile phones) where the communication originated or ended, can be located. They propose the following wording:

> "and where applicable, the geographical location in the telecommunications network where the communication originated or ended.."

12.2.1.15 The SAPS remarks that the non-exhaustive, more general definition is preferred. However, if a more technical definition could be proposed, it could be formulated as follows:

> "call-related information" includes details of dialling or signalling information that identifies in respect of -
>
> (a) a communication session:
> (i) the starting time for the session;
> (ii) ending time for the session;
> (iii) type of communication network;
> (iv) the source of the communication, namely whether audio, audio fax, audio modem, fax data, modem data, short message service or user to user communications are used;
> (v) where applicable, the geographical location in the telecommunications network where the call started or ended;
>
> (b) a call.
> (i) telephone number,

---

6 Chief Manager: Legal Component: Detective Service.

(ii) whether it is an incoming or outgoing call;
(iii) number of rings noted for incoming and outgoing calls;
(iv) the status signal sent to the dialling entity indicating whether a party is busy or disconnected;
(v) the dialled number recognition;
(vi) the calling number,
(vii) where applicable, the instrument or user identification number;
(viii) where applicable, the Short Message Service result;
(ix) mobile subscriber roaming number,
(x) the network from which the intercepted call originated;
(xi) subscriber number;"

12.2.1.16 Two Subcommittees of NICOC[7] (National Intelligence Co-ordinating Committee), namely the legal and technological committees[8] prepared a subsequent submission for the National Assembly Portfolio Committee on Justice which was made available to the Commission. The NICOC subcommittee points out that the proposed definition of "call-related information" does not distinguish between information applicable to cell phones and that which applies to fixed line telephones, it contains inaccuracies, in that even in the case of cellular calls it would not be possible to geographically locate the user, while it will only be possible to locate the origin of the call within the network (eg the cell from where the call originated or ended). The NICOC subcommittee remarks that the proposed clause should not be misunderstood as if it is imposing an obligation on service providers to keep information that would otherwise not be kept in the course of business. The NICOC subcommittee proposes the following clause:

> "Call-related information" means dialling or signalling information kept in the course of business by a person, body or organisation rendering a telecommunication service and which may include-
> (a) the origin, direction, destination, termination and duration of the communication;
> (b) equipment identification;
> (c) the geographical location in the telecommunication system where the communication originated or ended;
> of each communication generated or received by a user of any equipment, facility or service of a person, body or organisation rendering a telecommunication service.

12.2.1.17 The NICOC subcommittee further considers that the definition of "telecommunications line" should be considered. They point out that the definition in the principal Act was taken from the old Post Office Act of 1958 and that the definition does not

---

7 Hereinafter referred to as "the NICOC subcommittee".

8 Which represents the combined views of the Departments represented in NICOC, namely the SAPS, NIA, SASS and SANDF.

appear in the latter's successor, the Telecommunications Act of 1996, in which the term "telecommunication system" is defined. The NICOC subcommittee proposes that in order to provide for ever-changing technology, the term "telecommunications line", wherever it appears in the principal Act, should be replaced by the term "telecommunication system". They also propose that the definition of "telecommunication service" as it appears in the Bill, should be amended to read "any telecommunication service as defined in the Telecommunications Act, 1996".

12.2.1.18 Mr Harold Marshall[9] considers that the definition of call-related information will differ according to the type of service provided by the service provider and that required by the investigation officer. He asks whether the intention is that the Act should include radio communications as well and states that rural telephone systems use a combination of radio and telephone lines. He also refers to paging services and explains that paging services can be used for relaying messages and that some of the new systems are digital. Mr Marshall remarks that monitoring can be at different locations for different information.

12.2.1.19 Judge Gordon[10] comments that the proposed definition is adequate and correct. He notes that the draft follows the United States of America definition (Amendment to title 18 of U. S Code, Sec. 102 (2)). He states that he should mention that in the United States of America and Great Britain (GB), investigative Units make frequent use of Pen Registers and Trap and Trace devices in the above connection. No reference has, to his knowledge, been made to these devices in South Africa. He states that for the sake of completeness, in the event of these devices becoming available and used, the definition of "pen register" (Para 3.1.27 (3)), means "a device which records or decodes electronic or other impulses which identify the numbers dialled or otherwise transmitted on the telephone line to which such device is attached ... and, a "trap and trace device" means a device which captures the incoming electronic or other impulses which identify the originating member of an instrument or device from which a wire or electronic communication was transmitted". He notes that para 3.1.22 deals with the application for an order for both these devices.

---

9 Of Marshall International Sales whose products and services include electronic security, counter espionage equipment, surveillance systems, audio and video recording equipment, cctv equipment, telephone monitoring equipment, radio communications.

10 Office for the Control of Interception and Monitoring of Communications.

12.2.1.20 Messrs Paul Sheer, Anton de Wet, Tiaan van Schalkwyk, Francois Wolmerans and Philip Booysen of the company called Obsidian Systems state that computer Internet communication happens in a far more arbitrary, regular (i.e. often) and flexible way than traditional (eg telephonic) communication. They note that it is therefore sometimes difficult to determine when communication is explicitly requested between two parties or when it is occurring as a side effect of general computer operations, and that Internet communication is much easier to `wire-tap' than telephonic communication. They remark that eavesdropping is in many cases trivial and can even happen accidentally in the work of system maintenance. They consider that the legislature would have to address the issues of each of the many types of Internet communication. They note that in the case of Internet communications, the `Network/Service Provider' need not require special hardware facilities to monitor communications and that these facilities are available by default by virtue of the general flexibility of computer systems. They suggest that software facilities may be required, but then eaves-dropping *particular specific* communications *may* require software which does not exist and is prohibitively expensive to develop. They recommend that attention be given to the adoption of an Internet Communications Act. They consider that the Internet represents such a radical departure from traditional communications that it warrants a thorough investigation in itself.[11]

(c) Evaluation

12.2.1.21 The Commission considers that the American legal position is noteworthy when considering the definition of "call-related information". Judge Gordon pointed out the existence of pen registers in the USA in his comments to the Commission. Certain devices, when attached to a phone line, allow the numbers of incoming or outgoing calls to be recorded. A *pen register* is a device which records numbers dialled out on the telephone line to which it is attached. A *trap and trace device* records the numbers from which any incoming calls are dialled. According to federal[12] and Californian law, a court order must be obtained before these

---

11 See par 12.2.31.1 - 2 below where the issue of "hacking" is considered and where it is recommended that the matter of hacking and the broader issue of the desirability of legislation governing the Internet such as an Internet Communications Act should be dealt with in the Commission's investigation into computer related crimes (project 108) and not in this investigation.

12 Sec. 3121. (a) Except as provided in this section, no person may install or use a *pen register* or a trap and trace device without first obtaining a court order under section 3123 of this title or under

devices may be attached to a phone line. However, telephone companies may use these devices without a court order to protect against theft or fraudulent use of the telephone service or to protect customers from harassment. These devices may only be used to obtain the number of the calling party. The Digital Telephony Act of 1994 provides that pen registers and trap and trace devices may not be used to disclose the location of the calling party except to the extent that the location may be determined from the telephone number.[13] Information

---

the Foreign Intelligence Surveillance Act of 1978.
(b) The prohibition of subsection (a) does not apply with respect to the use of a *pen register* or a trap and trace device by a provider of electronic or wire communication service -
(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or
(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or
(3) where the consent of the user of that service has been obtained.
(c) A government agency authorized to install and use a *pen register* under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialling and signalling information utilized in call processing.
(d) Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

13 Sec. 1002.(a) Except as provided in subsections (b), (c), and (d) of this section and sections 1007(a) and 1008(b) and (d) of this title, a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of -
(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;
(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier -
(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
(B) in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);
(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and
(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects -

obtained from such devices must be limited to the phone number of the calling or called party.

12.2.1.22 It was noted in Chapter 1 above that the processing of personal data is regulated in the European Community by Convention no 108 of 28 January 1981,[14] Directive 95/46/EC of 24 October 1995[15] and that the protection of telecommunication data is particularly regulated by Directive 97/66/EC of 15 December 1997[16]. The terminology used in article 6(1) and (2) of the 1997 Directive regulating the processing of the data under discussion is noteworthy:

> 6(1) Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call without prejudice to the provisions of paragraphs 2, 3 and 4.
> (2) For the purpose of subscriber billing and interconnection payments, data indicated in the Annex may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued. [The list of data set out in the Annex is - data containing the number or identification of the subscriber station; address of the subscriber an the type of station; total number of units to be charged for the accounting period; called subscriber number; type, starting time and duration of the calls made and/or the data volume transmitted; date of the call/service; other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.]

12.2.1.23 The project committee considered the proposed definition and was of the view that the term "switching" should be included in the definition before the words "dialling and signalling". The committee considered that the provision is intended to be an inclusive provision and that the term "switching" should therefore be included in the proposed clause. The committee took the suggestion into account that call-related information should mean dialling or signalling information kept in the course of business by a person, body or organisation. The committee was of the view that this suggestion would unnecessarily restrict or limit the provision. The committee was of the view that the counter balance underlying the provision is the judicial safeguards where the applicant has to bring a good case to satisfy the judge that

---

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted;
and
(B) information regarding the government's interception of communications and access to call-identifying information.

14 Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data.

15 On the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data.

16 Concerning the Processing of Personal Data and Protection of Privacy in the Telecommunications Sector.

the requirements are met for him or her issuing a directive.

12.2.1.24 The Commission is of the view that Vodacom's suggestions on the purpose of the Act, namely that it is to provide for the monitoring of conversations, communications and postal articles and not ongoing surveillance, and the inclusion of the phrase "the location of the user at the time of the initiation or first reception of a call", in the definition, as well as the deletion of the words "*direction of a call*", are persuasive.

12.2.1.25 The Commission considers otherwise that the approach suggested by the project committee is persuasive and that the term "switching" should be inserted into the provision. The Commission is further of the view that the explanation by the NICOC subcommittee why the term "telecommunications line", wherever it appears in the principal Act, should be replaced by the term "telecommunication system" is persuasive and that the definition should be amended as suggested by NICOC.

(d) Recommendation

12.2.1.26 The Commission recommends that -

- the term "switching" should be inserted in the definition of "call-related information" and that the phrase concerning locational information be amended as Vodacom suggested to read as follows-

  "'call-related information' includes switching, dialling or signalling information that identifies the origin, destination, termination, duration and equipment identification of each communication generated or received by a customer or user of any equipment, facility or service rendered by a person, body or organization rendering a telecommunication service, and where applicable the location of such user at the time of the initiation or first reception of a call."

  and

(b) the definition "telecommunications line" should be replaced by the term "telecommunications system".

12.2.2 Clause 1(b): the definition of judge

(a) Comments on the proposed definition

12.2.2.1 Ms Hellen Naicker of the Department of Public Works considers that the substitution of the word Supreme Court with High Court is certainly acceptable and in line with the recent name changes to the Superior Court title.

12.2.2.2 The Law Society of SA's standing committee on constitutional affairs considers that retired judges should not be included in the definition of a "judge" in terms of clause 1 (b) because it may carry the risk of the appointment of a compliant judge, especially where the Minister of Justice designates the judge to perform the duties in terms of the Act.

12.2.2.3 The Office of the Director Investigating Directorate Organised Crime and Public Safety and the submission forwarded by the Director Public Prosecution of Cape of Good Hope comments as follows:

> Dit word aanbeveel dat alle regters, uitsluitende waarnemende regters, aangestel word vir doeleindes van hierdie Wet. Alternatiewelik beveel respondent aan dat elke Provinsiale en Plaaslike afdeling sy eie Regter kry wat vir doeleindes van hierdie wet aangestel word.
> Daar word dus deur respondent voorgestel dat die omskwywing van 'n Regter verbeter word om veral met verwysing na die Wet op Hooggeregshowe en enige ander wet wat 'n definisie ten opsigte van regters bevat, ten einde regsargumente in die verband uit te skakel.

(c) Evaluation

12.2.2.4 The Commission is of the view that the interpretational problems referred to by the Office of the Director Investigating Directorate Organised Crime is not very clear. It is also not particularly clear to the Commission which circumstances the Office has in mind which may lead to the question whether the judge exercising his functions under the Interception and Monitoring Prohibition Act is indeed a judge of the High Court. In the absence of clarity on these matters the Commission considers that there is no need to make it further clear in the Amendment Act that a judge acting under the Interception and Monitoring Prohibition Act acts under the authority of a judge of the High Court. The project committee and the Commission noted the suggestion that a retired judge should not be designated under the Act to consider applications. The project committee and the Commission do not agree that the designation of

a retired judge carries the risk of a compliant judge being designated. The Commission is of the view if the argument is to be consistent then the appropriate argument would be to insist that these judges be designated for example by the Chief Justice and not by the Minister of Justice who represents the executive.

(d) Recommendation

12.2.2.5 The Commission recommends that the definition of judge be amended as follows:

> "'judge' means any judge of any provincial or local division of the **[Supreme]** High Court of South Africa, including any judge discharged from active service under section 3 of the Judges' Remuneration and Conditions of Employment Act, 1989 (Act No 88 of 1989), and any retired judge, who is designated by the Minister of Justice to perform the functions of a judge **[within a particular division]** for the purposes of this Act."

12.2.3 Clause 1(c): serious offence

(a) Comments on the proposed definition

12.2.3.1 Ms H Naicker of the Department of Public Works notes that the current legislation defines a serious offence as an offence that is mentioned in Schedule I of the Criminal Procedure Act 51 of 1977, but with the following provisos:

i) that the offence is allegedly being or has been committed over a lengthy period of time;
ii) that the offence is allegedly being or has been committed on an organised basis, by the person or persons involved therein;
iii) that the offence is allegedly being or has been committed on a regular basis by the person or persons involved therein; or
iv) that the offence may allegedly harm the economy of the Republic

12.2.3.2 Ms Naicker remarks that the Department concurs with the view that is expressed by the Court in *S v Naidoo* that these offences will only be considered serious if the requirements of (i), (ii) and (iii) are met. She notes that these three paragraphs must be read disjunctively in order to give effect to the intention of the legislation. She states that if this section is to continue to exist in its present form, the grammatical construction of the section must be amended to include the words "or" or "alternatively" between the paragraphs. Ms Naicker

remarks that the individual paragraphs shall then be seen as separate requirements. She further considers that the requirements of a serious offence are unduly restrictive and would be an impediment in the investigation of serious crime in South Africa. She considers that the Act is deficient in that it does not include a list of possible crimes that should be included under serious offences. She is of the view that the exclusion of crimes such as once-off murder, robbery etc which are presently serious offences in South Africa worsens the situation.

12.2.3.3 Ms Naicker notes that before a crime of robbery would have to be considered a serious offence it would have to be committed regularly, over a lengthy period of time and have to be of an organised nature. She remarks that this scenario highlights the flaws in the definition. She considers that the words "lengthy period of time", "organised basis" and "regular basis" lack definition. She notes that the murder of 2 Ministers in separate incidents would therefore not rank as a serious offence because it was not committed over a lengthy period of time, it need not have been organised and it was not on a regular basis. She considers that the same analysis may be made in respect of a once-off spur of the moment robbery even if the amount of money stolen was approximately R 40 million, and that this crime would not even be considered under the present definition, if it were a robbery committed against a private sector. She notes that the robbery would fall into the definition if it affects the economy of the Republic therefore the robbery would have to be committed against an organ of the Public Sector.

12.2.3.4 Ms Naicker is of the opinion that the American approach would be a reasonable approach to adopt. She remarks that this approach lists various crimes that should be capable of being intercepted and monitored in order to obtain evidence of these crimes. She considers that due to the incredibly high crime rate in South Africa this needs to be addressed. Ms Naicker suggests that the following crimes should fall under the list of serious offences that would be capable of being monitored:

i) any offences relating to espionage, sabotage, treason or riots;
ii) any offences involving murder, kidnapping, robbery or extortion;
iii) any offence relating bribery of and corruption by public officials and witnesses, bribery in sport (Public Officials shall include State employees, Ministers of various departments and members of commissions etc.);
iv influencing or injuring a justice official, witness, obstruction of criminal investigations or obstruction of law enforcement;
iv) assassination and/ or kidnapping of the President and/or Presidential staff or ministers of the Cabinet;
vi) sexual exploitation of children;

vii) counterfeiting and fraud;
viii) drug offences;
ix) conspiracy to commit any of the above offences; and
x) any offence that affects the economy of the Republic.

12.2.3.5 Ms Naicker remarks that this is not an exhaustive list as the judge has the discretion to determine if the offence shall threaten the security of the Republic in that it affects the defence, economy, social welfare etc on a national level. She however considers that the use of the words "lengthy period of time" is problematic. She asks whether the crime then has to be committed over six months, twelve months or longer for it to be considered a lengthy period of time? She suggests that this clause be deleted altogether. She asks whether the investigating officer should consider that it is a lengthy period of time or would it have to be in the discretion of the judge? She remarks that these criteria should not be legislated upon but be seen as discretionary guidelines for the judges to assess. Ms Naicker considers that the South African judiciary has sufficient expertise to weigh the rights of the South African people against the intrusion by the State to determine what would amount to a reasonable infringement.

12.2.3.6 Ms Naicker notes that the same criticism applies equally to the use of the words "regular basis" and "organised basis". She asks whether the crime has to be committed with a certain degree of frequency or at what time intervals and whether three robberies in the space of a year would be sufficient or should it be three robberies in the space of three months for it to be on a regular basis. She notes that the criticism may seem harsh but the blanket requirement would hamper the investigation of crime, which is a major problem in the country. She considers that this element should rather be left to the discretion of the judge.

12.2.3.7 Ms Naiker suggests that the word "organised" may remain as a requirement but a definition should be attached to provide guidance to an applicant especially where the application is based on a criminal investigation.

12.2.3.8 MTN notes that the amendment proposes that the words "or other interest" be inserted in the definition. MTN is of the view that these particular words should not appear and should be deleted in their entirety. MTN considers that such "other interests" without being very clearly defined, could include the political interests on the government of the day. MTN is of the view that the addition of paragraphs (c), (d) and (e) would in any event cater for all criminal

activities that are perpetrated. Alternatively and as previously mentioned, MTN is of the view that the "other interests" should be very narrowly defined in the Act. MTN suggests that this would hopefully preclude any kind of governmental or political abuse that may be occasioned by the addition of the words "other interests".

12.2.3.9 The submission forwarded by the Director of Public Prosecutions of the Cape of Good Hope remarks as follows in this regard (as does the submission made by the Office of the Director Investigating Directorate: Organised Crime and Public Safety [IDOC]):

> Die Respondent ondersteun hierdie beoogde wysiging. Daar word egter voorgestel dat daar by paragraaf (a) tussen die Romeinse paragrawe (i) en (ii) aan die einde van elke paragraaf slegs die woord 'or' ingevoeg word ten einde die argument wat in Naidoo opgekom het vir eens en altyd te ruste te lê. Die invoeging van die beoogde definisie soos dit in die wysigingswetsontwerp op verbod op onderskepping en meeluistering voorgestel word, naamlik deur in artikel 1 ernstige misdade te omskrywe as die misdrywe vervat in Bylae 1 van die Strafproseswet word sterk ondersteun, aangesien daar in die verlede veral probleme ondervind is met die benutting van hierdie wet by misdrywe soos obsene telefoonoproepe, afpersing en telefoniese bomdreigemente.
> Die omskrywing van 'lengthy period' is egter meer problematies indien daar in gedagte gehou word dat 'lengthy period' baie relatief is tot die betrokke misdryf. So kan twee weke 'n lang periode wees waar iemand voortdurende obsene telefoonoproepe maak aan 'n sekere individu, maar terselfdertyd kan twee weke ook 'n baie kort periode wees waar daar byvoorbeeld te doen gekry word met dwelmhandel. Die voorstel deur die Respondent is dus dat 'lengthy period" iets is wat deur die betrokke verhoorhof bepaal moet word in elke geval.

12.2.3.10 Adv Mnyatheli of the Investigative Directorate Serious Economic Offences remarks that he is in agreement with the committee's view that reference to a lengthy period of time may present difficulties. He notes that it invites the question naturally whether there is no less intrusive manner in which the offence may be detected. He states that it may be pointed out also that logically an offence can be and usually is, describable as a serious offence even if it was not committed over a lengthy period of time. He considers that to suggest therefore a lengthy period of time as a criterion for the seriousness of an offence is to limit the exercise of detection, for example and to thwart the purpose of interception and monitoring. He suggests that *lengthy period of time* can be averred for instance in affidavit not as a criterion but as a motivation of the application before a judge. Adv Mnyatheli notes that that means therefore that it may not be necessary in every case and each case would be dealt with according to the merits it presents. He suggests that the circumstances of each particular case should be what fosters the application for a direction from a judge and that time and period should not be a

primary consideration. He suggests therefore that the reference to an offence having been committed over a lengthy period of time should be avoided and not made as an independent criterion.

12.2.3.11 Adv Mnytheli further states that in his view no harm is conceivable if the word interests of the Republic is used. He notes that if the interests are economic interests it is nothing bad to say so and the courts are used to the use of the term interests of the Republic. He thinks that the addition is necessary and any checks and balances may be gained by a judicial consideration, which will attend to each case on the basis of the merits it may present. He states that he has no problem with the use of the term.

12.2.3.12 The Law Society of SA's standing committee on constitutional affairs notes that the definition of "serious offences" in clause 1 (c) includes offences mentioned in Schedule 1 to the Criminal Procedure Act, 1977 provided that, *inter alia,* these offences may harm "other interests of the Republic" (clause 1 (c)(iii)). The reference to the "interests of the Republic" is reiterated in clause 3(b)(ii) when enumerating the grounds that need to be satisfied before a judge would issue a directive in terms of the Act. The Committee notes that case law is of little help in interpreting the ambit of this phrase. The Committee remarks that in *S v du Plessis* 1981 (3) SA 382 (A) at 383, the court had to interpret the phrase "interests of the Republic" in the context of the Official Secrets Act, 1956 and simply stated that whether something was "prejudicial to the safety or interests of the Republic is [a question] which must be objectively considered, having regard to all the relevant facts and circumstances". The Committee suggests that where the ambit of a law's application is difficult to define, it is too vague and may also be over broad (*R v Heywood* (1995) 24 CRR (2d) 189 (SCC) at 208). The Committee considers that virtually anything could be justified as being in the "interests of the Republic". The Committee submits that the phrase is too vague and ought to be deleted.

12.2.3.13 The SAPS[17] notes that it is appreciated that a very serious crime might be planned and executed during a short period. The SAPS states that as however it is pointed out in the Discussion Paper, the courts have interpreted the definition of serious crime by finding that the qualifications in paragraph (a)(i) - (iii) of the definition should be read disjunctively. The SAPS supports this interpretation. The SAPS remarks that the requirement relating to a long

---

17 Chief Manager: Legal Component Detective Services.

period of time is therefore not required over and above the other qualifications, and that they will not object to deleting paragraph (a)(i) of the definition in question.[18] The SAPS suggests that the interpretation of the definition could be easier if the word "or-"' could be inserted after subparagraph (i) and (ii), but it is believed that the drafting style is to insert it only before the last subparagraph.

12.2.3.14 Advocate JT Molefe notes that the project committee expresses a concern that the inclusion of "other interests of the Republic" might lead to abuse if an application is brought on such narrow grounds than for example "economic interests". He states that he however sees "interests of the Republic" as a fairly broad and at the same time limited concept for the following reason:-

> (a) An applicant will have to define these interests if a prima facie Case is to be made. This means that "interests of the Republic is not the unruly horse that the project committee fears it might turn out to be as the entire context of the Act, with the purpose being justifiable intrusion into a basic human right and prescriptive procedure will have a limiting effect.
>
> (b) The concept is on the other hand broad in the sense that the absence of limiting qualification such as "economic" makes for the possibility of dealing with any "interests" so long as they can be defined or particularised.

12.2.3.15 Advocate JT Molefe remarks that he sees no connection between the period of time over which an offence is being or has been committed and the length of time the monitoring is sought to take and considers that it maybe somehow implied. He states that he sees this as one of the restrictive provisos that are necessary in a law that makes serious inroads into the right of privacy and the economic freedom of service network providers. He would submit that it is even more necessary given the even more onerous duties imposed on service/network providers by the project committee's proposals. He notes that he does not see how the proviso can present difficulty where the applicant has to convince the judge that the offence cannot be properly investigated in another less intrusive manner. Advocate JT Molefe considers that on the contrary an applicant would need to have attempted or considered other methods of investigation over a period of some time in order to come to such a conclusion.

---

18 The NICOC subcommittee also proposes that the requirement that the offence is allegedly being or was allegedly been committed over a lengthy period of time, should be deleted.

12.2.3.16 The Cape Law Society's Criminal Law and Procedure Committee comments that with regard to the issuing of warrants, it is suggested that the English system should be applied, that is, warrants should be issued where necessary in the interest of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the country.

12.2.3.17 The Cape Law Society's Criminal Law and Procedure Committee suggests that the definition of "offence" could be improved by comparison with the Canadian Criminal Code.

12.2.3.18 Vodacom supports a broader definition of serious offences as proposed by the Commission. At the same, however, Vodacom submits that - contrary to the position reflected in clause 5B(4) of the draft Bill - it would be administratively preferable and more consonant with Constitutional principles, if requests for ongoing call-related data (which include locational information) were brought under this piece of legislation.

12.2.3.19 The SAPS[19] suggests that the words "organized crime" in the proposed definition of serious crime (paragraph (e)) be deleted. The reason is that paragraph (a)(ii) already refers to crimes committed on an organized, planned or premeditated basis. To again refer in paragraph (e) to organized crime, will create an interpretation problem and is an unnecessary duplication.[20] The SAPS considers furthermore that there should be a reference to conspiracy, incitement or attempt in respect of all the offences mentioned in the definition and not only in respect of paragraph (a).[21] The SAPS remarks that the offences of terrorism and sabotage (section 54(1) and (3) of the Internal Security Act, 1982) should be added to the definition of serious offence as paragraph (f).[22]

12.2.3.20 Judge Gordon[23] remarks that bearing in mind that investigations into a particular crime (or crimes) frequently lead to uncovering evidence of other - even unrelated crimes, he

---

19 Chief Manager Legal Component Detective Services.

20 The NICOC subcommittee also considers that in view of the wording of paragraph (a)(ii) namely organised, planned and premeditated crimes, the reference to organised crime in paragraph (e) seems to be a duplication and should be deleted in paragraph (e).

21 The NICOC subcommittee also supports this proposal.

22 This proposal is also supported by the NICOC subcommittee.

23 Office for the Control of Interception and Monitoring of Communications.

considers that the requirement in the proposed definition that the *offence concerned is being or has been committed over a lengthy period of time* is unnecessary and in fact may be counter-productive to investigation. He accordingly recommends that this requirement be deleted for purposes of the Bill.

12.2.3.21 Mr Harold Marshall states that the wording of the provision is vague. He considers that the Act should cover all crimes and not only 'serious crimes' and that this will allow the Judges or others to avoid having to study definitions. He suggests that all crimes are serious and that many companies are affected by matters that may not be classified as serious crimes but are considered detrimental to the running of the company and its people. Mr Marshall notes that industrial espionage may or may not be considered as a serious crime in the eyes of the state but it can be devastating to the organisation concerned. He believes that the present definitions and discussion paper are mainly concerned with crimes that will affect the government, the country or the economy. He proposes that consideration should be given to the protection of companies and individuals.

12.2.3.22 Mr Marshall is of the view that the wording "serious offences" be changed to "criminal offences". He considers that any crime that carries a conviction can be included and that we are going to rely on people with integrity to issue directives and should give them the scope to decide. He notes that he can not see a list being prepared that will cover all the different crimes and their time periods being workable and to the satisfaction of Investigating Officers.

(b) Evaluation

12.2.3.24 The project committee considered that there is no need that the provision should require that the offence "is allegedly being or has allegedly been committed over a lengthy period of time". The committee resolved that subparagraph (i) should be deleted and that the other subparagraphs should be renumbered. The committee noted the suggestion made by a respondent that the phrase "including any conspiracy, incitement or attempt to commit any offence" should apply in regard to all the offences set out in the provision and decided that the phrase should be moved to follow after subsection (e) in order to apply as was suggested and that the words "of the above-mentioned offences" should be substituted for the words "any offence referred to in that Schedule". The committee further considered that the words "by the

person or persons involved therein" contained in subsection (e) is tautologous since it is clear that the person concerned is involved in the offence. The committee therefore resolved that these words be deleted. The committee noted that it was suggested in written comments that the words "other interests of the Republic" may depend on party political considerations and should be reconsidered. The committee is was, however, not persuaded by this suggestion.

12.2.3.25 The Commission agrees with the reasoning adopted by the project committee and recommends that the provision be amended as suggested by the project committee. The Commission however considers on the issue of "the other interests of the Republic" that the proposed wording is too vague and that provision should be made for "other compelling national interests of the Republic". The Commission also considers that the provision should be amended by the substitution of the words "any offence relating to organized crime, money laundering or the proceeds of crime" with the words "any offence referred to in the Prevention of Organised Crime Act, 1998".

(c) Recommendation

12.2.3.26 The Commission recommends that the definition of serious offence be amended to read as follows:

"'serious offence' means -

(a) any offence mentioned in Schedule I to the Criminal Procedure Act, 1977 (Act No. 51 of 1977), **[including any conspiracy, incitement or attempt to commit any offence referred to in that Schedule,]** provided that -

[(i) **that offence is allegedly being or has allegedly been committed over a lengthy period of time];**

[(ii)] (i) that offence is allegedly being or has allegedly been committed on an organized, planned or premeditated basis **[by the person involved therein]**; or

[(iii)] (ii) that offence is allegedly being or has been committed on a regular basis **[by the person or persons involved therein]**; or

[(iv)](iii) that offence may allegedly harm the economy or other compelling national interests of the Republic; or

(b) any offence referred to in sections 13 (f) and 14 (b) of the Drugs and Drug Trafficking Act, 1992; or

(c) any offence relating to the trafficking in firearms, ammunition and explosives; or

(d) any offence relating to the death or serious bodily harm of any person; or

(e) any offence referred to in the Prevention of Organized Crime Act, 1998;

or

(f) any offence threatening the security of the Republic;

including any conspiracy, incitement or attempt to commit any of the above-mentioned offences.

12.2.4 Clause 1(d): telecommunication service

(a) Comments on the proposed definition

12.2.4.1 The submission forwarded by the DPP Cape of Good Hope states the following in this regard:

> Ten opsigte van hierdie definisie is dit raadsaam om daarop te let dat die gebruik van 'n selfoon in Amerika gesien word as die uitsaai van inligting en is daar regspraak wat daarop dui dat 'n individu nie kan staatmaak op sy reg van privaatheid wanneer hy 'n selfoon gebruik nie, aangesien daardie inligting die hemelruim ingestuur word en dit gehoor kan word deur enige persoon wat die korrekte aparaat besit.
> 'n Verdere aspek wat in gedagte gehou sal moet word ten opsigte van die monitering van selfone ingevolge hierdie wet is die aspek dat huidige wetgewing meld dat die Regter van die Provinsie van waar die boodskap versend word of die Regter van die Provinsie waar die boodskap ontvang word of waarskynlik versend of ontvang sal word, magtiging ingevolge hierdie wet sal kan verleen. Die vraag ontstaan egter wat gebeur in die gevalle waar 'n persoon byvoorbeeld in die Wes-Kaap woonagtig is, die selfoon daar aankoop maar die selfoon gebruik in die Vrystaat vir iemand wat hy skakel in Kwa Zulu Natal. Sal die moniteringsspan nou geregtig wees om ook daardie gesprek mee te luister of sal dit ongemagtigde meeluistering wees aangesien dit gedoen is buite die afdeling van die regter van waar die boodskap of inligting versend is of waar dit ontvang is? In die verband word daar voorgestel dat daar 'n bepaling in die onderhawige wet geplaas word wat sal lees dat waar die ondersoekbeampte aansoek doen om meeluistering te doen op 'n selfoon, dit irrelevant is van waar die gesprek versend of van waar dit ontvang is en dat alle sodanige inligting wat versend of ontvang is op die gemagtigde selfoon toelaatbaar sal wees in 'n kriminele vervolging teen enige relevante party.

12.2.4.2 Adv Mnyatheli of the Investigative Directorate Serious Economic Offences considers that the proposed definition is a good one as it captures the main conventional services that are readily understood to be telecommunication services. He suggests that because large strides have and continue to be made in the line of technological development that an all-embracive definition be opted for. He states that it is noted that the suggested definition reflects, with the exception of reference to mobile or fixed telecommunication service, to a large degree the nature of the licence of the national fixed line operator, being Telkom. He considers that one of the spin-offs of the dynamism inherent in the telecommunication

development is the inevitable aspect of convergence of technologies, i.e. the telecommunications and the broadcasting technologies to be found for example in video conferencing. He considers that while we may readily say that a television broadcasting which connects people from different corners of the world is a broadcasting service, it might be interesting to note that it is unachievable without a telecommunications facility. Adv Mnyatheli remarks that the convergence of these technologies is integral to the advancement of communication services and a definition therefore of telecommunication service must need to take that into account. He proffers the following definition:

> Telecommunication service shall mean any telecommunication service as defined in the Telecommunications Act including but not limited to the following-
>
> (a) a public switched telecommunication service;
> (b) a mobile or cellular telecommunications service;[24]
> (c) a national long distance telecommunication service;
> (d) an international telecommunication service;
> (e) a satellite telecommunication service;
> (f) Value-added network services in which are included any electronic data interchange, Email, protocol conversion access to a data or managed data network service and any video conferencing or communication; or
> (g) Any other telecommunication service licensed as such in terms of the Telecommunications Act.

12.2.4.3 SATRA states that it is their contention that the proposed definition, taken from the Telecommunications Act does not adequately define a 'telecommunication service', particularly insofar as e-mail, electronic data interchange, voice mail, telecommunication related publishing and advertising services whether electronic or print, video communications and voice over the Internet are concerned. SATRA suggests that the definition should be augmented to some extent. They note that SAT'RA has had first hand experience with the conundrum of applying the current definition of telecommunication services. SATRA remarks that, in terms of the Telecommunications Act, it has dealt with e-mail, electronic data interchange, video conferencing and the like in terms of section 40 of the Telecommunications Act. SATRA states that although the term 'Value-added network services' is not specifically defined it can be inferred these are VANS and the argument can then be made that these are not telecommunication services as per the definition. SATRA considers that e-mail electronic date interchange etc are licenced as VANS and not telecommunication services so the catch-all

---

24 He notes that he is not happy with the suggested wording "fixed cellular service".

phrase in (c) of the definition may not remedy the situation.

12.2.4.4 SATRA states that notably the Telecommunications Act definition does not make particular mention of the point-to-point aspect of telecommunications. SATRA has found this aspect useful in distinguishing telecommunication services from other services. SATRA remarks that the definition of 'communication' in section 5 of the Australian Telecommunications Act 1991 may prove useful in drafting a more technically correct definition. SATRA points out that the relevant definitions read as follows:

> "Communication" includes any communication;
> (a) whether between persons and persons, things and things or persons and things; and
> (b) whether:
> (i) in the form of:
> (a) speech, music or other sounds; or
> (b) data; or
> (c) text; or
> (d) images, whether or not animated; or
> (e) visual
> (f) signals; or
> (g) in any other form or in any combination of forms.

12.2.4.5 SATRA notes that definitions contained in the United States of America's Communication Assistance for Law Enforcement Act (1994) should also be considered for inclusion in the definition to make it as definitive as possible. SATRA refers to the terms 'electronic messaging services' and 'information services':

> The term 'electronic messaging services' means software-based services that enable the sharing of data, images, sound, writing or other information amount computing devices controlled by the senders or recipients of the messages
> and
> The term 'Information services'
> (A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing or making available information via telecommunications; and
> (B) includes
> (i) a service that permits a customer to retrieve stored information from, or file information for storage in information storage facilities;
> (ii) electronic publishing; and
> (iii) electronic massaging services

12.2.4.6 The Joint Communication Security Council and the SA Communication Security

Agency states that their one of their main concerns about the effects of the proposed amendments are whether it is intended that Internet Service providers fall under the Act. They consider that Internet Service Providers (ISPs) cannot, in their opinion, be classified as any of -

- a public switched telephone network;
- a mobile or fixed cellular telephone service;
- a national long distance telecommunication service;
- an international telecommunication service; or
- a telecommunication service licensed as such in terms of the Telecommunications Act, 1996.

12.2.4.7 They note that Discussion Paper 78 gives the impression that it would like to see e-mail and video communications (and digitised telephony via the Internet, presumably), and therefore, ISPs, covered by the provisions of the Act. They note that it would, one presumes, involve some sort of control/licensing of ISPs. They remark that should this be done, the following should be borne in mind:

- Any tapping of the communication channel can only be done at the ISP: the architecture of the Internet is such that packets belonging to the same data stream do not necessarily follow the same routes.
- The intercepted data stream will be a bitstream (at the rate of Kilobits or even Megabits per second) representing text, graphics, digitised voice, header information, etc as well as possibly ciphertext. It will be extremely difficult, though probably not impossible, to separate the "interesting" parts of the bitstream from the remainder.
- Even if only the source and/or destination of the data stream are required, anonymous remailers can be used to hide these.
- The cost of providing interception/monitoring facilities may well be such that most of the smaller ISPs will be forced to stop operating.
- Awareness by the public that their ISPs are providing access to their communications will have a very deleterious effect upon the development of electronic commerce.

12.2.4.8 Vodacom considers that the proposed definition of "telecommunication services" is technically incomplete. They consider, for example, that section 40 of the Telecommunications Act, 1996, with respect to value added network (VANs) licensing should be noted. Vodacom suggests that even if all telecommunication systems or services are eventually to be brought within the ambit of the Interception and Monitoring Prohibition Act, the requirement to obtain monitoring and interception devices or equipment should not be imposed on all types of operators immediately. Vodacom considers that, initially, only the Telkom public switched telecommunication network and the mobile cellular operators should provide monitoring facilities. Vodacom submits that given the potential impact on the development of

the telecommunications industry and the price of telecommunication services in the republic, as well as the potential negative impact on the financial performance of various telecommunications enterprises, the decision to request such facilities, devices and services of Internet service providers and other VANs, satellite service operators and other licensees should be made by the Minister of Telecommunications in consultation with the South African Telecommunications Regulatory Authority (SATRA) and the Minister of Justice. Vodacom further suggests that if it proves necessary to require the provisioning of such facilities under clause 5(6) and (7) of the draft Bill, the Minister shall be required to follow an appropriate administrative law procedure, including a hearing with the affected licence holder. Vodacom considers that it should be noted that any amendments to the terms and conditions of existing licences should be effected in accordance with the terms of those licences and the Telecommunications Act of 1996. Vodacom also submits that if the existing provisions of the Act allowing for "reasonable remuneration" are retained, and the requests for such facilities are at once technically feasible and commercially reasonable, there should be no reason to invoke such measures.

12.2.4.9 Telkom notes that the Telecommunications Act defines "telecommunication service" as "any service provided by means of a telecommunication system", and that the Act does not provide explicit definitions of the services listed in the proposed definition, except for the mobile cellular services of Vodacom and MTN and the Public Switched Telecommunication Service of Telkom. Telkom states that it should be noted that there is no mention in the Telecommunications Act of a "fixed cellular telecommunication service'. Telkom considers that the proposed definition in the Draft Bill reflects some, but not all telecommunications services permissible in terms of the Telecommunications Act. Telkom suggests that it would therefore be preferable in accordance with the definitions provided by section 34(2) to state that:

> 'telecommunication service' means any telecommunication service as defined in the Telecommunications Act, 1996 (Act No. 103 of 1996), in respect of -
>
> (a) a public switched telecommunication service;
> (b) a mobile **[or a fixed]** cellular telecommunication service;
> (c) a national long distance telecommunication service;
> (d) an international telecommunication service; or
> (e) any other telecommunication service licensed or deemed to be licenced or exempted from being licenced as such in terms of the Telecommunications Act, 1996.

12.2.4.10 The SAPS[25] remarks that it is important that a roleplayer, such as the Department of Communications and Telkom indicate whether it is in agreement with the proposed definition. The SAPS notes that the proposed definition follows more or less the wording of the Telecommunications Act, 1996, in respect of the definition, in that Act, of *"telecommunication* service". They state that according to informal discussions with Telkom, it appears as if there is unlicenced, but legal operators. The SAPS notes that it is believed that this aspect will be dealt with by Telkom in their submission to the Law Commission. The SAPS further states that the Interception and Monitoring Prohibition Act, 1992, was specifically amended during 1998, in the Judicial Matters Amendment Act, 1998, to ensure that all types of communications, namely fax, e-mail, etc. may be intercepted and that the obligation be created in regard to telecommunication service providers to assist in executing directions in respect of not only *"conversations"* but also *"communications".* The SAPS remarks that it is, however, appreciated that the definition of *"telecommunication service"* should be correct and inclusive and the Department of Communications and Telkom might assist in that regard.

(b) Evaluation

12.2.4.11 The project committee considered the suggestions made by the respondents and resolved that Telkom's proposal in respect of a mobile or fixed cellular telecommunication service be followed in order to tally with the wording of the Telecommunications Act, namely the deletion of the words "or a fixed" in paragraph (b). The committee also considered it appropriate that paragraph (e) of the proposed definition should be amended, as proposed by Telkom, who suggests that the definition "telecommunication service", be further defined as follows, namely "and any other telecommunication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Telecommunications Act, 1996" . The committee added a caveat that although it decided on the suggested definition proffered by Telkom, regard should be had to conformity with the definitions contained in the Telecommunications Act.

12.2.4.12 The Commission considered the amendments suggested by respondents and the project committee and agrees with the project committee that the definition of telecommunication service should be amended as suggested.

---

25 Chief Manager Legal Component: Detective Services.

12.2.4.13 The Commission also noted the suggestion that there is a need to define "communication". The Commission notes that the Act was amended as recently 1998 by the insertion of the phrase "or conversations" in the definitions of "monitor"and "monitoring device" and in sections 2(1)(b) and (c) and 5(1)(a) and the phrase "conversation or" in section 4(2)(a) to make it clear, as the SAPS pointed out, to ensure that all types of communications, namely fax, e-mail, etc. may be intercepted and the obligation be created in regard to telecommunication service providers to assist in executing directions in respect of not only *"conversations"* but also *"communications"*. The Commission is of the view that this aspect could be made much clearer if the Act were to include the following definition, namely "'communication' includes conversation and a message, and any part of a conversation or message, whether in the form of speech, music or other sounds, data, text, visual images, whether or not animated or signals or in any other form or in any combination of forms".

(c) Recommendation

12.2.4.14 The Commission recommends that the definition of telecommunication service be amended by the deletion of the words "or a fixed" in paragraph (b) in the phrase "of a mobile or fixed cellular telecommunication service" in order correspond to the wording of the Telecommunications Act. The Commission also considers it appropriate that paragraph (e) be amended as proposed and recommends the following wording, namely "and any other telecommunication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Telecommunications Act, 1996" .

12.2.4.15 The Commission further recommends that the definition contained in the Australian Telecommunications (Interception) Act defining "communication" be included in the Act, and, as a consequence of the proposed definition of "communication" which includes conversations, references to "conversations" be deleted throughout the Act .

12.2.5 Clause 2(1)(b): no person shall intercept or monitor any conversation or communication

(a) Comments on clause 2(1)(b)

12.2.5.1 It was proposed in the discussion paper that section 2 of the Interception and Monitoring Prohibition Act, be amended by the substitution for paragraph (b) of subsection (1)

of the following paragraph:

> '(b) intentionally monitor any conversation or communication, without the knowledge or permission of the parties to such conversation or communication, by means of a monitoring device so as to gather confidential information concerning any person, body or organisation."

12.2.5.2 Telkom states that it should be noted that on a customer's request, Telkom will monitor call data on the customer line. (Detail billing with respect to outgoing calls from the customer line, in particular the duration of calls, numbers dialled and the costs thereof, however, the conversation is not monitored). Telkom explains that this, in effect, means that call data is monitored at the request of and with the knowledge of only one of the parties to the communication. Telkom suggests the following amendment:

> "(b) Intentionally monitor any conversation or communication, without the knowledge or permission of at least one of the parties to such conversation or communication, by means of a monitoring device, so as to gather confidential information concerning any person, body or organisation."

12.2.5.3 Vodacom proposes in its June submission that the Act should only refer to "communication" and that all references to "conversations" should be deleted in the Act in order to avoid "hair-splitting" legal disputes. Vodacom notes that an SMS or e-mail is like a telegram, ie it is *dispatched* without the certainty of a reply which a conversation would require, a call to a person's cell phone may result in a conversation, but if the call is routed to voicemail, will result in something more like a telegram and it is questionable whether two computers *converse* in the course of a data communication. M-Web states that the Act does not define with sufficient clarity what the difference is between "communications, conversations", and 'confidential information'. M-Web considers that if any communication is to be the subject of interception or monitoring then in order for any law to pass constitutional muster, such communication must be capable of clear definition.

12.2.5.4 MTN notes that the suggested amendment proposes that the phrase "without the knowledge or permission of the parties to such conversation or communications" be inserted in the current Monitoring Act. They consider that the proposed wording would therefore not allow any person to record a conversation with any other party with the intent to gather confidential information. MTN states that as an example, where a person receives a nuisance or abusive phone call, the proposed wording will not allow for the receiver of such

abusive phone call to record such conversation to be used for judicial proceedings. MTN remarks that the suggested wording would oblige the receiver of the abusive phone call to firstly request permission from the abuser to record whatever such abuser is about to say and that this would clearly defeat the purpose of such recording. It is therefore suggested by MTN that the proposed clause be suitably amended.

12.2.5.5 The SAPS[26] notes that the provisions of Act 127, as well as the proposed amendment to section 2(b), is aimed at prohibiting the monitoring of conversation or other forms of communications by a person or persons other than the parties taking part in the conversation. The SAPS notes that the Act contains no provision prohibiting a party to the conversation to monitor, ie record, the conversation. The SAPS further states that if, however, the participant records the conversation with the intent to gather confidential information and to enable a person or person who are not party to the conversation to monitor (listen to the recording) the conversation, then section 2(b) of Act 127 is contravened. The SAPS remarks that a perfect example of such a contravention is where the police sends an agent to a suspect with the intent to gather evidence against such suspect and directs the agent to record the conversation. The SAPS points out that direct intent to gather confidential information by means of monitoring (recording) the conversation is present and a contravention of section 2(b) is evident and the agent is an accomplice to this contravention.

12.2.5.6 The SAPS consider that the intent can also be indirect. The SAPS states that the intention is to record only your own remarks to enable a person to monitor your words whilst knowing full well that the words of the other party to the conversation will also be recorded and monitored by the person not party to the conversation. The SAPS states that the third possibility is where the intent can be imputed because of an awareness of possibility *(dolus eventualis).* The result, which is the monitoring of the conversation, is not intended but foreseen as a possibility by the person making the recording and he reconciles himself with the possibility of such monitoring possibly taking place. The SAPS notes that the admissibility of a recording or evidence gained as a direct result of a recording where the recording was made by a participant to the conversation (hereinafter referred to as participant monitoring) is another issue which also is not addressed by the Act or proposed amendments. Firstly, because the recording might constitute a criminal act the admissibility can be disputed under the principle

---

26 Office of the Commander Technical Support Unit Eastern Cape.

of "fruits of the poisoned tree'. Secondly convincing Constitutional arguments can be shown which supports the non-admissibility of recordings made by means of participant monitoring where the State is a party. The SAPS suggests that urgent attention must be given to amend Act 127 in such a manner that it provides for lawful participant monitoring. The SAPS considers that a system which provides for a magistrate or judge to grant permission for participant monitoring on the same principles and criteria as applicable in the application for a search warrant should satisfy the applicable Constitutional norms and values.

12.2.5.7 The NICOC subcommittee supports explicit provision for excluding participative surveillance from the prohibition on monitoring. They propose that section 2(1) be amended to follow the wording of the United States legislation to read as follows: "intentionally monitor any conversation or communication by means of a monitoring device, without the knowledge or permission of one of the parties to such conversation or communication, so as to gather confidential information concerning any person, body or organisation." They further propose, in view of this proposal and the recent judgement of the High Court in *S v Kidson* that the words "or with" be deleted in section 2(1)(c) as follows: "... conversations by **[or with]**, or communications to or from, a person, body or organisation, whether a telecommunication**[s]** **[line]** system is being used in conducting those conversations or transmitting those communications or not, be monitored in any manner by means of a monitoring device". The National Intelligence Agency[27] remarks that for purposes of clarity "all" could be inserted before the word "parties".

12.2.5.8 The DPP Investigating Directorate Organised Crime and Public Safety and the DPP Cape of Good Hope comments as follows in this regard:

> Respondent stem met hierdie wysigings saam, maar beveel aan dat dit duidelik gemaak moet word dat waar 'n party tot die gesprek die opname maak, daardie persoon nie 'n misdryf pleeg nie en ook nie magtiging in terme van hierdie wet benodig nie. Dit moet ook duidelik gemaak word in die wetgewing dat hierdie wet slegs van toepassing is op derde party monitoring, dit wil sê monitoring deur 'n party wat nie 'n party is tot die gesprek nie.

12.2.5.9 Advocate JT Molefe remarks that the interpretation of the present provision is that the "knowledge" or "consent" of one party to an intercepted/monitored communication or

---

27 The Deputy Director-general: Operational Services.

conversation creates immunity from prosecution. He states he doubts whether an intrusion of this sort without judicial authority can pass the test of constitutionality. He considers that prudence seems to suggest that even where one of the parties to a conversation or communication "consents" or has "knowledge" of the intrusion, such intrusion must be preceded by judicial authorisation. He notes that this approach would also limit constitutional challenges to evidence obtained in this fashion.

12.2.5.10 Judge Gordon[28] remarks that he agrees with the amendment to section 2(1)(b) of the Act, relating to monitoring. He considers that the general position as regards **interception** i.e. party interception between A and B, is clear and requires no further clarification. He points out that possible queries may arise in regard to **monitoring** with the emphasis, now suggested, by the added phraseology, where prohibition might apply to a face to face monitoring, i.e. between A and B direct. He states that he regrets to say that the example suggested in 10.8.1 of monitoring between a police agent and the leader of an **infiltrated** syndicate is not clear to him. If the infiltrated leader is part of the police operation, the fact that the recording is unaffected by prohibition is self-evident. The act of monitoring may invariably exclude third party surveillance and he thinks it might be helpful if he refers to the United States of America and Great Britain positions in regard to:

1. A police agent who communicates with a suspect ordinarily subject to prohibition, if he monitors the conversation.

2. A private person at the behest of a police agent, (or privately), who performs the acts subject to prohibition.

In the United States of America:

As to (1) above, Judge Gordon quotes from the FB1 Electronics Surveillance Manual:

"Neither Title III (equivalent to our Sec 127) nor the Fourth Amendment prohibits a law enforcement officer or a person acting under colour of law from intercepting a wire, or electronic communication without a court order when one of the parties to the communication has consented to the interception".

As to (2) above: Monitoring by Private Parties:

"Under 18 U. S. C., an individual may intercept an oral, wire or electronic communication if that person is a party to the communication or a party to the communication has given consent, provided the interception was not made for a criminal or tortuous purpose".

---

28 Of the Office for Interception and Monitoring.

12.2.5.11 Judge Gordon states that the position in Great Britain is in effect much the same. He remarks that section 2 of the Intercept Act provides that the prohibition does not apply if a person by or to whom the communication is sent has reasonable grounds for believing that the person sending the communication has consented to the monitoring. Judge Gordon considers that in his view, as regards the law enforcement officer (police), the suspect he interviews becomes a party to the communication - and consensual monitoring takes place. The prohibition does not apply and no judicial direction is required. However, the private person, *if the purpose is to obtain information for a criminal or tortuous purpose* would require the requisite approval. Consent, in such a case cannot be justified or implied. Judge Gordon does not recommend inclusion of these matters by way of amendment to the Act. He would suggest that when necessary they be included in the Rules.

12.2.5.12 The SAPS[29] welcomes the proposal that participative surveillance be excluded from the prohibition on monitoring. They state that participative surveillance, undertaken in consultation with Directors of Public Prosecutions, without directions for monitoring and as part of investigations in terms of section 252A of the Criminal Procedure Act, 1977, forms the backbone of many organized crime investigations countrywide. Directors of Public Prosecutions all over the country have expressed from time to time the opinion that no direction is needed for participative surveillance. The SAPS notes that in many countries participative surveillance without a direction is allowed to take place. They state that it is agreed fully with the Project Committee that the present Act allows participative surveillance, without a direction. It is also agreed that the Act should be made more clear on this aspect. The proposed wording of section 2(1)(b), however, presents a problem, if it is interpreted that all the parties to the conversation have to give their permission. It is proposed that it reads, as in the United States legislation, namely intentionally monitor any conversation or communication, *without the knowledge or permission of one of the parties to such conversation or communication*, by means of a monitoring device so as to gather confidential information concerning any person, body or organization.

12.2.5.13 The SAPS suggests that it is important to amend section 2(2)(c) as follows:

---

29 Chief Manager: Legal Component Detective Services.

"'(c) conversations by **[or with]** a person, body or organization, whether a telecommunications line be monitored is being used in conducting those conversations or not, in any manner by means of a monitoring device."

12.2.5.14 Adv Deon van Wyk advises that he was instructed by a client to prepare an opinion on the legality of voice logging. He states that voice-logging is the recording of telephone calls. The Wordnet system supplied by his client, can simultaneously record various calls digitally. The system also allows for an elaborate system of searching and tracing various calls recorded. The system is a "telecommunication equipment or facility", approved by SATRA in terms of section 54 of the Telecommunications Act. He states that it is of interest to note that the following is specified in the *Functional Requirements for Automatic Answering and Recording Equipment* in terms of SATRA -TE-002 under the heading recording of conversations:

"2.1 Recording of the conversation by participants
Recording of two way telephone conversations by any one of the participants in a telephone conversation is permitted, provided that the recording equipment has been approved by SATRA for connection to the network.
2.2 Recording of the conversation by third party
The recording of a private telephone conversation by an outsider or third party not taking part in the actual conversation, constitutes an actual invasion of the privacy of the individual and is therefore an unlawful deed as well as a criminal act."

12.2.5.15 Adv Van Wyk states that the activities his clients are involved in can mainly be categorized as follows:

- Emergency services:

The telephone calls are typically recorded for reasons of verification, traceability and identification to be used in a command and control environment. It is also used for the later construction of incidents. Typically the users include the SA Police, Fire departments and Ambulance services.

- Treasury operations:

These include the logging of all voice communications in a dealing room of a financial institution. They trade in all financial instruments via the telephone, excluding equities. The voice recording is used as the final arbiter of the spoken word. Typically users include the banking sector.

- Equity dealers:

The functions of the logging are similar to those of the treasury operations, however the clients mainly deal in equities, derivatives and futures. The current users include a number of stock broking firms.

- Tele-insurance: (Short and long term):

Voice logging is used to record telephone calls of customers who take out policies, as well as submit claims, via the telephone. As information is provided that will determine the policy costs, the underwriting risk as well as claim details, it is imperative that recordings of the telephone conversations are available. Claims are paid out or repudiated based

on what was said. The current users include insurance institutions.

- Tele-banking:

Customers can do virtually all their banking transactions via the telephone, such as transfers, stopping of cheques, etc. This of course can lead to fraud or disputes as relating what was said and who gave instructions. The banks require voice recordings to protect both themselves and their clients. The users include banks.

- Telemarketing (Non-financial):

These include the selling of products advertised mainly on television where clients can buy various types of products by submitting and paying with their credit cards. The contracts are invariably oral and the only proof of the contract is the recording.

- Call centres: Recorded messages is used for agent assessment, training and alike functions.
- Utilities:

Used for the later construction of incidents. Typically the users include the SA Police, Fire departments and Ambulance services.

- Treasury operations:

These include the logging of all voice communications in a dealing room of a financial institution. They trade in all financial instruments via the telephone, excluding equities. The voice recording is used as the final arbiter of the spoken word. Typically users include the banking sector.

- Equity dealers:

The functions of the logging are similar to those of the treasury operations, however the clients mainly deal in equities, derivatives and futures. The current users include a number of stock broking firms.

- Tele-insurance:

(Short and long term): Voice logging is used to record telephone calls of customers who take out policies, as well as submit claims, via the telephone. As information is provided that will determine the policy costs, the underwriting risk as well as claim details, it is imperative that recordings of the telephone conversations are available. Claims are paid out or repudiated based on what was said. The current users include insurance institutions.

- Tele-banking:

Customers can do virtually all their banking transactions via the telephone, such as transfers, stopping of cheques, etc. This of course can lead to fraud or disputes as relating what was said and who gave instructions. The banks require voice recordings to protect both themselves and their clients. The users include banks.

- Telemarketing (Non-financial):

These include the selling of products advertised mainly on television where clients can buy various types of products by submitting and paying with their credit cards. The contracts are invariably oral and the only proof of the contract is the recording.

- Call centres:

Recorded messages is used for agent assessment, training and alike functions.

- Utilities:

The users are mainly electricity departments who record calls between customers, the control centre as well as the technical staff on the ground.

12.2.5.16 Adv Van Wyk remarks that the situation is that the clients of his client and other users of voice logging systems conclude literally billions rands worth of transactions over the telephone, with little or no paper. The only record of such transactions lies in the recording by

the voice logger. He states that in the modern age of technology and commerce, where time is of the essence, telephonic contracts are the order of the day. People invariably trade on stock exchanges by telephone. Institutions that demand written (paper) contracts could soon become marginalised. The clients purchase and maintain their voice logging systems at a fairly substantial cost. To replace such systems would be very costly. If voice logging is prohibited the clients not only possibly face criminal prosecutions, but also and more importantly, civil suites by hundreds or thousands of clients for alleged breach of privacy. They might also end up with the situation that having to find out, at a crucial stage in expensive litigation, that not only is the recording illegal, but also inadmissible in a Court of Law. This refutes exactly the rationale behind the implementation of the voice logging system in the first place. It is of utmost importance to the users of voice logging systems that they have legal certainty. He states that the current legal position is far from clear. He refers to the case of *S v Kidson*[30] where Cameron J remarked as follows:

> "(a) The principle of interpretation *infavorem libertatis* obliges the conclusion that the prohibition in section 2(1)(b) of the 1992 statute applies in the first instance only to third party monitoring of conversations. Its primary signification is not to cover participant monitoring, i.e. when one of the parties to the conversation monitors it.
> (b) Police, defence and intelligence agency personnel who wish to monitor conversations for the purpose the statute specifies must however in terms of sections 2(2) and 3 obtain authorisation even for participant monitoring.
> (c) A private individual who with the assistance of the police engages in participant monitoring is in the absence of proof that the operation is a sham designed to evade the statutory prohibition not covered by the criminal prohibition."

12.2.5.17 Adv Van Wyk also remarks that careful study of the *Kidson* case and the case of *Protea Technology Ltd. and Another v Wainer and Others* [1997] All SA 594 clearly shows the lack of clarity of the provisions of Act 127 of 1992. He suggests that if the comments of McCall J in *S v Naidoo and Another* 1998 (1) All SA 189 (D&C) is also taken into account, the need for reform by the legislator becomes apparent. He proposes the insertion of a section 2(3) explaining that such an amendment, or words to the similar effect would, in his view, ensure that the spirit of the Constitution, both as to the right to privacy and right to free economic activity, be adhered to and that he does not feel it is necessary to define any of the words or phrases contained in the proposed section 2(3), as it would unfairly inhibit the Courts to interpret the proposed section.

---

30 1999 (1) SACR 338 (W).

"The interception or monitoring of a communication or conversation, not made for the purpose of committing an offence, or delict, or causing other injury, by a party to such a communication or conversation, is not prohibited, if-

(a) the party is not acting under the colour of law, and

the purpose of the interception or monitoring is the making or preserving of an record of the communication or conversation; or

(b) if the interception or monitoring, is made unsurreptitiously in the normal course of business.

12.2.5.18 The Banking Council of SA also points out that there are many instances where telephone conversations are recorded, for good business reasons in case of a subsequent dispute over the exact content of an instruction given over the telephone. The Banking Council notes that typical cases are money market dealing rooms (where verbal buy-sell instructions are given and received; the exact time is also recorded), telephone banking, telephone short term insurance quotations and purchase orders etc. The Banking Council notes that there is a lacuna in existing law relating to this important business practice. The Banking Council recommends that the new legislation specifically makes provision for these practices - where one party to a telephone discussion records the discussion, for valid business purposes, between himself and other parties.

12.2.5.19 Mr Marshall considers that there are aspects in the proposed provision that need clarification. He sets these aspects out as follows:

(1) Third party interception and monitoring is carried on by persons outside the conversations with a view to obtaining information or evidence of a crime being committed or planning to be committed. Without a directive, this is illegal.

(2) Monitoring and recording a conversation, should not be illegal if one of the parties taking part in the conversation, is aware of the recording of the meeting or conversation. This is very often necessary in some cases, for the protection of the individual. The person may be aware that he will be approached and offered a bribe or invited to participate in a crime. This can not be investigated by the Police until after the event has occurred. This recording can then be used for further investigation or prosecution and should be accepted as evidence. There a number of scenarios to which this situation could be applied.

(3) Interception and monitoring by the legal occupier of premises, which takes place on the premises of the legal occupier, should not be prohibited.

A situation now exists where a company can install a surveillance video camera on their premises. The video is acceptable as court evidence of a crime but if audio is also recorded of the crime, then the audio is illegal. This is wrong. Many crimes start at company premises. Staff may use the company's time,

> telephone or fax to plan a crime. There is presently no recourse to the owner to prevent the crime or to prosecute or even dismiss. The owners would have to wait for a number of crimes to have been committed before they can lay charges and the waiting time will obviously cost them money. Only then does it become a serious crime, according to the present amendment.

12.2.5.20 Mr Marshall notes further that an important recurring problem with call-related information is the reception of unwanted abusive or similar phone calls. He notes that the investigation of this type of offense has been a problem in the past and that, at the present moment, Telkom will not investigate a case unless an alleged crime has been reported to the Police and a docket has been opened. He points out that an application for investigation must be made by the Police and that the SA Police at the moment are overburdened with more serious cases. He considers that they do not have the manpower to handle this type of complaint and proof of the offence thereby rests with the complainant who has no recourse to the equipment required to monitor the calls. Mr Marshall considers that when the phone call is incoming, the caller has already given up their right to privacy by initiating the call and that the complainant is one of the parties to the call and should have the right to record the call. He notes that technology is now available for a device to be installed on the receiving telephone which will register the calling party identification (Caller ID). Mr Marshall points out that in other countries, this device is freely available and is also used as a screening device to restrict incoming calls and maintain privacy. He suggests that in order for the device to work, the authorities must program their system to provide the information and that Telkom can provide this facility on all electronic exchanges. Mr Marshall notes also that the cellphone service providers already have this facility installed if the call originates from another cellphone and that this facility can be of great importance in matters such as bomb threats, abusive calls and including unwanted civil abuse. It will play a very important role in the case of emergency services where the caller can be identified easily and especially where they are incapable of talking coherently. He proposes that this feature should be incorporated in the regulations to be available from the service provider.

12.2.5.21 The SAPS[31] recommends that the following definition be inserted in section 1 of the Act:

> "'Private communications' means any communication (including oral conversations)

---

31 Chief Manager Legal Component Detective Services.

made under circumstances in which it is reasonable for a party to it to expect that it will not be intercepted/monitored by a person other than a party to the communication, even if any party to it suspects that it is being intercepted or monitored by such a person."

(b) Evaluation

12.2.5.22 The project committee considered the question of what it is that is sought to outlaw by the Act. The committee noted that it was initially considered that the permission or knowledge of one party to the conversation is adequate and that the committee was of the view initially, as was stated in the discussion paper, that what is aimed at was getting the permission of both or all the parties to the conversation or communication. The committee noted the suggestion by the SA Police Service that the requirement should be that the permission or knowledge of one party suffices.

12.2.5.23 The project committee noted the rider contained in the section namely the monitoring of any conversation or communication "so as to gather confidential information". The committee considered that if someone tapes an abusive phone call it is not done for the purpose contemplated in the Act, and if a detective tapes a conversation with an informant it is not done to gather confidential information. The committee considered that the aim of the prohibition contained in the Act is to prohibit what is colloquially referred to as eavesdropping or phone tapping and that the prohibition is not aimed at someone taping his or her own phone calls. The committee took into account that although it might be unethical, it is a different matter whether it is intended to be unlawful. The committee took into account that the court in the case of *S v Kidson*[32] grappled with the interpretation of the Act in circumstances where the Police made use of an informer using a recording device to record a conversation with Mrs Kidson the nature of which was incriminating. There was an attempt in the case to argue that the recording was unlawful in the light of the prohibition contained in the Act and that it should be excluded for the reason of the discretion to exclude unlawfully obtained evidence. The committee noted that the court had to apply the section as it currently is and that it is broadly stated, ie the permission or knowledge by one or both parties to the conversation is not required.

12.2.5.24 The committee was of the view that it is obviously clear that the aim of the Act

---

32 1999 (1) SACR 338 (W).

is to outlaw the listening in to other people's conversations unless one has obtained the prescribed authority. The committee posed the question why would the prohibition not apply, or why should it not apply if a person were to initiate a call and is making a recording with the aim to gather confidential information, although it would seem not to have been the intention of the provision. It seemed to the committee that the intention is to outlaw third party monitoring or non-participative monitoring. The committee noted that there is an innovation in the provision in the sense that subsection (1)(a) uses the word intercept which carries the connotation of, as it were, an outsider which enters into the picture, whereas subsection (1)(b) uses the word "monitor". The committee considered that one could therefor have the situation where, for example a police trap or a police informer goes in with a recording device and there is a third party, ie the Police at a base station or whatever, who are monitoring the conversation. The committee noted that the recording would be permissible as a matter of law for the agent who went in to give first hand evidence of what the person said to him or her, but bizarrely the most accurate recoding of what actually occurred, would be outlawed. The committee considered that it would be consistent with the judgment in the *Kidson* case if the committee were to say that what is illegal is where both parties to the conversation are ignorant to the interception of their conversation by a third party. The committee noted that one is hesitant to make it more difficult for law enforcement but considered that what the section refer to as "confidential information" squarely concerns the commission of a crime and that is what law enforcement wishes to listen in to. The law enforcement agencies do not want to establish whether someone is ie having an affair. The committee considered that what the provision is concerned with is information relating to a serious offence or the security or interests of the country.

12.2.5.25 The committee considered that it might well be confidential information if one wants to know where the suspect is going to be and that although he or she is committing a crime but his private movements are, for example, that he or she is going to be in hotel X, and once the crime element is taken out, it is information about his private life. The committee was of the view also that since no one suggested that the wording "so as to gather confidential information" should be deleted, they should be retained. The committee considered that the words "between two or more persons without their knowledge or permission" should be inserted in section 2(1) (b). The committee was of the view, furthermore, that it should not try to attempt to expand or explain "confidential information" but would rather leave it to judicial interpretation.

12.2.5.26 The Commission noted the Case of *R v Duarte*[33] heard by the Canadian Supreme Court where the court held as follows:

> The principal issue in this appeal is whether the commonly styled "consent" or "participant" surveillance i.e., electronic surveillance in which one of the parties to a conversation, usually an undercover police officer or a police informer, surreptitiously records it - infringes the right under s. 8 of the Charter to be secure against unreasonable search and seizure. This raises the subsidiary issues of whether such infringement is justifiable under s. 1 of the Charter and whether the recorded conversation can nonetheless be admitted into evidence against an accused. I should at the outset note that "consent surveillance" is an unhappy term to describe a practice where only one party to a conversation has agreed to have it recorded. As put by the United States Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967), at p. 358: "the very nature of electronic surveillance precludes its use pursuant to the suspect's consent." I shall, therefore, use the term "participant surveillance".
>
> The importance of the issues can hardly be gainsaid. Carr, The Law of Electronic Surveillance, points out, at pp. 3-61, that in the United States this mode of surveillance is without question "the most widely used and most frequently practiced [sic] mode of eavesdropping". Though I have found no data on the relative frequency of this practice in Canada, the cases would indicate that it is also widespread here. The extensive use of electronic surveillance in this country is documented. The Law Reform Commission of Canada's working paper on Electronic Surveillance reports at p. 10 that on a relative basis, Canadian law enforcement authorities request twenty times more authorizations to conduct electronic surveillance than their American counterparts.
>
> ...
>
> The Risk Analysis of the Court of Appeal
>
> In upholding the legality of participant surveillance, the Court of Appeal relied heavily on American authorities, citing several decisions of that country's Supreme Court, notably *United States v. White*, 401 U.S. 745 (1971), a plurality decision which has been interpreted as giving that court's imprimatur to the practice, though the specific legislative provisions authorizing it were not directly placed in issue; see Carr, op. cit., at pp. 3-62. Cory J.A., at p. 390, accurately summarized the logic of those decisions as resting on the notion that "the consent to the interception by the recipient may be looked upon as no more than an extension of the powers of recollection of the recipient of the communication". In essence, the starting point for the analysis is the proposition that the person who divulges any confidence always runs the risk that his interlocutor will betray the confidence. As Cory J.A. put it, at p. 393: "The expression of the idea and the assumption of the risk of disclosure are therefore concomitant."
>
> The argument is then developed by pointing out that disclosures of this nature have always been admissible in a court of law. It is but a small step to the conclusion that constitutional expectations of privacy would therefore not operate to prohibit the interception of conversations which one of the participants is surreptitiously recording. As Cory J.A. put it, at pp. 393-94:
>
> > Given that it is accepted that the informant may testify in this manner as to pertinent conversations, the admission of electronic recordings of those conversations would seem to be a reasonable, logical and sequential step in trial proceedings. In this regard, the accurate transcript of the conversation should so often benefit the accused as the informant.

---

33 Accessed at http://www.droit.umontreal.ca/doc/csc-scc/en/pub/1990/vol1/html/1990scr1_0030.html on 3/8/99 case reference [1990] 1 SCR.

...

Stripped to its essentials, petitioner's argument amounts to saying that he has a constitutional right to rely on possible flaws in the agent's memory, or to challenge the agent's credibility without being beset by corroborating evidence that is not susceptible of impeachment. For no other argument can justify excluding an accurate version of a conversation that the agent could testify to from memory. We think the risk that petitioner took in offering a bribe to Davis fairly included the risk that the offer would be accurately reproduced in court, whether by faultless memory or mechanical recording. [Emphasis added.]

The decision in *Lopez v. United States* proceeds on the basis that participant surveillance is inherently less offensive than third party surveillance because the agent of the state hears nothing that his interlocutor did not intend him to hear. As the court there put it, at p. 439:

> ... the device was used only to obtain the most reliable evidence possible of a conversation in which the Government's own agent was a participant and which that agent was fully entitled to disclose. And the device was not planted by means of an unlawful physical invasion of petitioner's premises under circumstances which would violate the Fourth Amendment. It was carried in and out by an agent who was there with petitioner's assent, and it neither saw nor heard more than the agent himself.

Thus, for the Court of Appeal, inasmuch as the police are subjected to no warrant requirement in their use of informers or in their efforts to insinuate themselves into the confidence of a suspect, the use of electronic surveillance, as an adjunct to that process, is of no constitutional significance. In other words, if there has been a violation of privacy on the part of the state, it is complete when the confidence of the person under suspicion is gained. The Charter cannot purport to protect us if we don't know how to choose our "friends".

In summary, the risk analysis that is at the heart of the Court of Appeal's judgment rejects the notion that any distinction grounded on constitutional concerns should be drawn between evidence gained through the testimony of a participant to a conversation, and evidence gained through a surreptitious electronic recording of that conversation. A person who has voluntarily chosen to confide his wrongdoing to another, and who, by happenstance, has had the misfortune (from his perspective) of doing so in the presence of a microphone, should not be able to invoke the Charter to prevent divulgation of the confidence in a court of law. Incriminating statements and confessions of wrongdoing are not per se constitutionally protected communications; provided the accused spoke of his own free will, there is no constitutional significance to be accorded the manner in which the evidence was gained. In effect, the court chose to treat the risk that an interlocutor will divulge one's words and the risk that he will make a permanent electronic record of them at the behest of the state as being of the same order of magnitude.

This argument is not without weight: the fact that it counts among its adherents the Supreme Court of the United States and many state appellate courts testifies to that.

The Opposing Approach

With respect, it seems to me, the Court of Appeal failed to deal with the true issue raised in this appeal. The real question, as I see it, is whether our constitutional right to be secure against unreasonable search and seizure should be seen as imposing on the police the obligation to seek prior judicial authorization before engaging in participant surveillance, or whether the police should be entirely free to determine whether circumstances justify recourse to participant surveillance and, having so determined, be allowed an unlimited discretion in defining the scope and duration of participant surveillance. This Court is accordingly called on to decide whether the risk of warrantless surveillance may be imposed on all members of society at the sole discretion of the police.

...

It should come as no surprise that these parties shied away from engaging in such an unequal contest. *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, instructs us that the primary value served by s. 8 is privacy, and, as I noted in *R. v. Dyment*, [1988] 2 S.C.R. 417, at p. 426, the spirit of s. 8 must not be constrained by narrow legalistic classifications. If one is to give s. 8 the purposive meaning attributed to it by *Hunter v. Southam Inc.*, one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance and to which, in consequence, the protection accorded by s. 8 should be more directly aimed, an issue I shall more fully develop as I go along.

Not surprisingly, then, the Crown sought to focus more sharply on participant surveillance and to draw a distinction between it and other types of electronic surveillance. If that endeavour is to succeed, however, one must proceed on the assumption that the factors that support the imposition of a requirement for an authorization in the third party interception (i.e., non-participatory surveillance) of private communications hold no currency where participant surveillance is concerned. This proposition takes one back to the rationale for the regulation of electronic surveillance generally, and I shall now deal with it at greater length.

The rationale for regulating the power of the state to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it (see definition section of Part IV.1 of the Code) has nothing to do with protecting individuals from the threat that their interlocutors will divulge communications that are meant to be private. No set of laws could immunize us from that risk. Rather, the regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.

The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in United States v. White, supra, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.

This is not to deny that it is of vital importance that law enforcement agencies be able to employ electronic surveillance in their investigation of crime. Electronic surveillance plays an indispensable role in the detection of sophisticated criminal enterprises. Its utility in the investigation of drug related crimes, for example, has been proven time and again. But, for the reasons I have touched on, it is unacceptable in a free society that the agencies of the state be free to use this technology at their sole discretion. The threat this would pose to privacy is wholly unacceptable.

...

I am unable to see any logic to this distinction between third party electronic surveillance and participant surveillance. The question whether unauthorized electronic surveillance of private communications violates a reasonable expectation of privacy cannot, in my view, turn on the location of the hidden microphone. Whether the microphone is hidden in the wall or concealed on the body of a participant to the conversation, the assessment whether the surreptitious

recording trenches on a reasonable expectation of privacy must turn on whether the person whose words were recorded spoke in circumstances in which it was reasonable for that person to expect that his or her words would only be heard by the persons he or she was addressing. As I see it, where persons have reasonable grounds to believe their communications are private communications in the sense defined above, the unauthorized surreptitious electronic recording of those communications cannot fail to be perceived as an intrusion on a reasonable expectation of privacy.

The Charter standard just described must, in my view, apply on a uniform basis. To have any meaning, it must be taken to afford protection against the arbitrary recording of private communications every time we speak in the expectation that our words will only be heard by the person or persons to whom we direct our remarks. Section 8 of the Charter guarantees the right to be secure against unreasonable search or seizure. Our perception that we are protected against arbitrary interceptions of private communications ceases to have any real basis once it is accepted that the state is free to record private communications, without constraint, provided only that it has secured the agreement of one of the parties to the communication. Since we can never know if our listener is an informer, and since if he proves to be one, we are to be taken to be tacitly consenting to the risk that the state may be listening to and recording our conversations, we should be prepared to run this risk every time we speak. I conclude that the risk analysis relied on by the Court of Appeal, when taken to its logical conclusion, must destroy all expectations of privacy.

I am unable to see any similarity between the risk that someone will listen to one's words with the intention of repeating them and the risk involved when someone listens to them while simultaneously making a permanent electronic record of them. These risks are of a different order of magnitude. The one risk may, in the context of law enforcement, be viewed as a reasonable invasion of privacy, the other unreasonable. They involve different risks to the individual and the body politic. In other words, the law recognizes that we inherently have to bear the risk of the "tattletale" but draws the line at concluding that we must also bear, as the price of choosing to speak to another human being, the risk of having a permanent electronic recording made of our words.

The risk analysis relied on by the Court of Appeal fails to take due account of this key fact that our right under s. 8 of the Charter extends to a right to be free from unreasonable invasions of our right to privacy. The Court of Appeal was correct in stating that the expression of an idea and the assumption of the risk of disclosure are concomitant. However, it does not follow that, because in any conversation we run the risk that our interlocutor may in fact be bent on divulging our confidences, it is therefore constitutionally proper for the person to whom we speak to make a permanent electronic recording of that conversation. The Charter, it is accepted, proscribes the surreptitious recording by third parties of our private communications on the basis of mere suspicion alone. It would be strange indeed if, in the absence of a warrant requirement, instrumentalities of the state, through the medium of participant surveillance, were free to conduct just such random fishing expeditions in the hope of uncovering evidence of crime, or by the same token, to satisfy any curiosity they may have as to a person's views on any matter whatsoever.

In summary, the question whether to regulate participant surveillance cannot logically be made to turn on the expectations of individuals as to whether their interlocutor will betray their confidence. No justification for the arbitrary exercise of state power can be made to rest on the simple fact that persons often prove to be poor judges of whom to trust when divulging confidences or on the fact that the risk of divulgation is a given in the decision to speak to another human being. On the other hand, the question whether we should countenance participant surveillance has everything to do with the need to strike a fair balance between the right of the state to intrude on the private lives of its citizens and the right of those citizens to be left alone.

This is the manner in which the issue has been framed in the American appellate decisions that have rejected *United States v. White*, supra, in interpreting rights to privacy in state constitutions.

The reasoning in these decisions, in my respectful view, provides a complete answer to the view that the risk posed by the divulgation of the informer, and that posed by letting the agents of the state, at their whim, surreptitiously record private communications to which they are privy, are risks of the same order. These decisions make an eloquent case in support of the proposition that unregulated participant surveillance cannot be reconciled with the right to be secure against unreasonable search and seizure.

State Appellate Decisions Rejecting *United States v. White*

I turn first to a decision of the Supreme Court of Alaska in *State v. Glass*, 583 P.2d 872 (1978), in which the court, in interpreting that state's constitutional right to privacy, held that a person who engages in a private conversation is entitled to assume that his words will not be broadcast or recorded, absent his consent or the existence of a warrant. In reaching his decision, Boochever C.J. quoted at length from the dissenting judgment of Hufstedler J. in *Holmes v. Burr*, 486 F.2d 55 (1973). In the latter case, one Marburger had permitted his telephone conversation with Holmes to be recorded. Hufstedler J., at pp. 71-72, makes the initial observation that it is aberrant to import the notion of risk in assessing the constitutionality of "participant" surveillance:

> This doctrine, relied upon by the majority in the case at bench, is a hybrid of factual and fictitious elements and of individual and societal judgments. If Holmes knew that his conversation might be electronically intercepted by the government, or if warrantless electronic monitoring were so pervasive that he is chargeable with such knowledge, a factual foundation would exist for invoking the venerable assumption of the risk doctrine. However, if he did not know and if he had no reason to be aware of the risk, that doctrine is inapt. To say that a person "assumes the risk" of electronic surveillance, although he was rightfully oblivious to the risk, is to mislabel a newly created rule of law limiting the scope of the Fourth Amendment.

In a perceptive passage, Hufstedler J. goes on to point out, at p. 72, the fallacy of arguing that the risk of exposure by the "tattletale" and the risk of surreptitious recording are one and the same:

> Repetition of conversations thought to be confidential is a known risk. However, the risk that one's trusted friend may be a gossip is of an entirely different order than a risk that the friend may be transmitting and recording every syllable. The latter risk is not yet rooted in common American experience, and it should not be thrust upon us: the differences between talking to a person enswathed in electronic equipment and one who is not are very real, and they cannot be reduced to insignificance by verbal legerdemain. All of us discuss topics and use expressions with one person that we would not undertake with another and that we would never broadcast to a crowd. Few of us would ever speak freely if we knew that all our words were being captured by machines for later release before an unknown and potentially hostile audience. No one talks to a recorder as he talks to a person. [Emphasis added.]

The Superior Court of Pennsylvania in *Commonwealth v. Schaeffer*, 536 A.2d 354 (1987), has also held that warrantless electronic surveillance violates that state's constitutional right to be secure from unreasonable searches and seizures. Cirillo J., who also takes direct aim at the assumption of risk doctrine, points out, at p. 365, that it destroys our right to fix the limits of publicity we choose to give our remarks. He states:

> A person committing his views "to the sight of his friends" knows he risks misjudging his friends, but he doesn't forfeit the right to determine in the first place to whom he will directly speak. The body bug destroys that right of self-determination, and if people in society come to believe the practice is widespread and done without probable cause, they may begin to fall silent on many occasions when previously they would have felt free to speak, confident in the belief that they could challenge the credibility or memory of the

> trusted colleague who would betray them.

In my view, the above remarks demonstrate the fallacy of the conclusion that the risk of being recorded is simply a variant of the risk of having one's words disclosed by the person to whom we speak. Surreptitious electronic recording annihilates the very important right to determine to whom we speak, i.e., the right to choose the range of our auditors. As pointed out by Cirillo J., at p. 365, in the case of participant surveillance, a speaker no longer has any choice whether to disclose his private thoughts to the government. Rather, he is compelled to do so. As he notes, at p. 365:

> Every speaker knows and accepts as a "condition of human society" that his listener may go to the police, but he does not intend by speaking to give up the right to exclude the police from his home. But if the police are simultaneously recording every word, they are already there, in the home, uninvited, contrary to every reasonable expectation that most people in society still have.

Implicit in the arguments in support of "consent" surveillance, it seems to me, is the notion that a man has no one but himself to blame if he is confounded by his own words. Thus, if someone is imprudent enough to reveal his wrongdoing, it makes no sense that the law discard that evidence just because the wrongdoer spoke into a microphone. There is a serious flaw in this argument. It rests on the assumption that the relevant inquiry is limited to the legitimate expectations of privacy of "criminals". But, again, the real question raised by this appeal lies elsewhere. As put by the Massachusetts Supreme Court in *Commonwealth v. Thorpe*, 424 N.E.2d 250 (1981), at p. 258: "the relevant question is not whether criminals must bear the risk of warrantless surveillance, but whether it should be imposed on all members of society".

In Commonwealth v. Schaeffer, supra, at p. 366, Cirillo J. concedes that there might be room for complacency were the sole effect of warrantless surveillance to compel criminals to engage in self-censorship. But inasmuch as the very premise of a warrantless procedure is that the police can engage in the practice at their sole discretion, any sanguinity in this matter is misplaced. Harlan J. in his dissent in *United States v. White*, supra, makes the point that the implications in allowing warrantless surveillance cannot be narrowly circumscribed. He stated, at p. 789:

> ... it is too easy to forget -- and, hence, too often forgotten -- that the issue here is whether to interpose a search warrant procedure between law enforcement agencies engaging in electronic eavesdropping and the public generally. By casting its "risk analysis" solely in terms of the expectations and risks that "wrongdoers" or "one contemplating illegal activities" ought to bear, the plurality opinion, I think, misses the mark entirely. On Lee does not simply mandate that criminals must daily run the risk of unknown eavesdroppers prying into their private affairs; it subjects each and every law-abiding member of society to that risk. [Emphasis added.]

Harlan J. went on to make the seminal observation that the imposition of a warrant requirement would have the sole effect of ensuring that police restrict "participant monitoring" to cases where they can show probable cause for a warrant. It is unclear to me how compelling the police to restrict this practice to instances where they have convinced a detached judicial officer of its necessity would hamper the police's ability effectively to combat crime. But even if this were so, this restriction would be justified by the knowledge that the police would no longer have the right "to train these powerful eavesdropping devices on you, me, and other law-abiding citizens as well as the criminal element", to cite the observation of Cirillo J. in *Commonwealth v. Schaeffer*, supra, at p. 367. The appellant put the matter trenchantly in his factum:

> A warrant requirement simply ensures that when the undercover agent goes in with the potential to make a permanent, electronic record of the conversation that takes place, it will be one that should be recorded (a proposed drug sale), as opposed to one that should not (the suspect's sex life or his views of the government).

In summary, I think, with respect, that Cory J.A. fails to give due weight to the policy implications of allowing the police to conduct warrantless surveillance when he states, at p. 394, that "it is only those whose conversations are concerned with various illegal activities who will be seriously concerned about the possibility of their remarks being recorded". On the contrary, the decision whether to allow or disallow this practice is fraught with the gravest of implications. To countenance this practice would not strike only at the expectations of privacy of criminals and those concerned with wrongdoing. Rather, it would undermine the expectations of privacy of all those who set store on the right to live in reasonable security and freedom from surveillance, be it electronic or otherwise. And it has long been recognized that this freedom not to be compelled to share our confidences with others is the very hallmark of a free society. Yates J., in *Millar v. Taylor* (1769), 4 Burr. 2303, 98 E.R. 201, states, at p. 2379 and p. 242:

It is certain every man has a right to keep his own sentiments, if he pleases: he has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends.

If this Court is to give its imprimatur to the practice of warrantless electronic surveillance, the words of Harlan J., dissenting in *United States v. White,* supra, at pp. 787-89, may fairly be said to apply:

> Authority is hardly required to support the proposition that words would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed. Were third-party bugging a prevalent practice, it might well smother that spontaneity - reflected in frivolous, impetuous, sacrilegious, and defiant discourse - that liberates daily life. Much off-hand exchange is easily forgotten and one may count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record. All these values are sacrificed by a rule of law that permits official monitoring of private discourse limited only by the need to locate a willing assistant. [Emphasis added.]

The Undermining of Part IV.1 of the Code

The appellant raises the additional point that dispensing the police from the requirement to seek a warrant for conducting participant surveillance effectively allows the police to do indirectly what Part IV.1 of the Code prohibits them from doing directly. Faced with the choice of having to seek a warrant, and being able to proceed without one, it can reasonably be expected that they will, circumstances permitting, elect to proceed without one.

Here, the police, acting without any judicial authorization, wired an apartment for a period of some two years, installed listening devices in another location, and employed an automobile location beeper. In circumstances such as these, where the police have evidence of a conspiracy and have elicited the services of an informer, can there be any compelling reason to suggest that the interests of justice would not be better served by requiring the police to attend before a superior court judge to obtain an authorization as opposed to letting the police be the sole arbiters of the scope of the investigation and its duration?

It is worth noting, in this regard, the basis for the conclusion of Martin J.A. in *R. v. Finlay and Grellette*, supra, that Part IV.1 of the Code is constitutional. While he was ready to accept that the interception of private communications does constitute a search and seizure within the meaning of those terms as they are used in the Charter, he concluded that such searches and seizures, when authorized in accordance with the requirements of Part IV.1 of the Code, would ordinarily be reasonable precisely and solely because the provisions and safeguards of Part IV.1 preclude the police from embarking on fishing expeditions in the hope of uncovering evidence of crime.

With regard to these safeguards it is worth remembering that Part IV.1 of the Code:

(a) stipulates that authorizations for electronic surveillance are only to be given on a showing that there is no real practical alternative (s. 178.13(1)); in other words, as put by the Ontario Court of Appeal in *R. v. Playford* (1987), 40 C.C.C. (3d) 142, at p. 185: "... it is treated as a last resort investigative mechanism", and can only be obtained for investigation of the most serious offences in the Code (s. 178.1);

(a) sets strict time limits on authorizations (s. 178.13(2)(e));

(c) prescribes that a judge may include any conditions and restrictions that he considers advisable in the public interest;

(d) authorizes renewals only on a showing of cause and a detailing of all interceptions made prior to the request for the authorization and the number of previous authorizations;

(e) mandates that notification be given to the person whose communications have been intercepted (s. 178.23(1));

(f) requires the Solicitor General of Canada to prepare a comprehensive report on all electronic surveillance conducted pursuant to authorizations (s. 178.22(1));

(g) engages the responsibility of the Attorney General of the province in which the application is sought, or of the Solicitor General (or duly appointed agents) (s. 178.12(1)); and

(h) provides that authorizations may only issue on the order of a superior court judge (s. 178.12(1)).

If the constitutionality of Part IV.1 of the Code is predicated on the numerous safeguards designed to prevent the possibility that the police view recourse to electronic surveillance as a humdrum and routine administrative matter, it would seem anomalous that participant surveillance, which leaves to the sole discretion of the police all the conditions under which conversations are intercepted, should be held to meet the definition of "reasonable" in the context of s. 8 of the Charter. I think that the appellant makes a good point when he submits that the large-scale police investigative activity using participant surveillance for monitoring and recording private conversations effectively by-passes any judicial consideration of the entire police procedures and thereby makes irrelevant the entire scheme in Part IV.1 of the Code.

As was put by Martin J.A. in *R. v. Finlay and Grellette*, supra, at p. 70:

> Authorizing such a serious intrusion on the individual's reasonable expectation of privacy as the interception of his private communications on the basis of mere suspicion would not further the interests of the administration of justice, but would bring it into disrepute.

Section 1 Justification

It is necessary to make only brief mention of possible justification under s. 1 of the police action in this case. The question whether participant surveillance constitutes a reasonable limit on the right to be secure against unreasonable search or seizure takes one back to the point that the appellant is in no way arguing that the police should be denied the right to use informers or to intercept communications themselves once they have gained the confidence of a suspect. The sole thrust of his argument is that judicial supervision of the practice should exist, just as it exists in the case of third party surveillance. In a word, there is no justification for warrantless searches once it is accepted that the police could employ the same investigatory tool with or without a warrant. This simple fact (and I find no argument by the respondent refuting the notion that the police could have attended before a judge to secure an authorization for participant surveillance) destroys, in my view, any argument that participant surveillance can be upheld as a reasonable limit to the right to be secure from unreasonable search and seizure.

To conclude, the Charter is not meant to protect us against a poor choice of friends. If our "friend"

> turns out to be an informer, and we are convicted on the strength of his testimony, that may be unfortunate for us. But the Charter is meant to guarantee the right to be secure against unreasonable search and seizure. A conversation with an informer does not amount to a search and seizure within the meaning of the Charter. Surreptitious electronic interception and recording of a private communication does. Such recording, moreover, should be viewed as a search and seizure in all circumstances save where all parties to the conversation have expressly consented to its being recorded. Accordingly the constitutionality of "participant surveillance" should fall to be determined by application of the same standard as that employed in third party surveillance, i.e., by application of the standard of reasonableness enunciated in *Hunter v. Southam Inc.*, supra. By application of that standard, the warrantless participant surveillance engaged in by the police here was clearly unconstitutional.

12.2.5.27 The Commission also considered the decision by Cameron J in the case of *S v Kidson*[34]. The court considered whether a recording and transcript of a conversation between a suspect called Rabane and a potential accused, made covertly by the suspect, with the assistance of the police, was admissible against the accused in subsequent criminal proceedings. It was submitted in the case that the Interception and Monitoring Prohibition Act does not apply to a conversation monitored by one of the participants to the communication. The court remarked that the North American courts refer to this as participative surveillance and that it is contrasted with third party surveillance, where an outsider monitors or surveils the conversation of two other parties. The court noted the State's argument that if the prohibition of the Act was interpreted absolutely it would mean that every person who records his or her own telephone conversation for the purpose commits an offence and that section 2(1)(b) should therefore be read as prohibiting only third party monitoring. The court remarked as follows[35]:

> In my view the legislature can not have intended to impose an unqualified prohibition on participant monitoring. The preamble to the Act states its purpose as being "to prohibit ... the monitoring of *certain* conversations' only (my emphasis). A total prohibition was therefore not envisaged, and in my view the limitation lies not only in the purpose for which the monitoring is undertaken ('to gather confidential information'), but also in the parties to the conversation which is monitored. The legislature's primary purpose seems to have been to protect confidential information from illicit eavesdropping. ... The most natural signification of eavesdropping is third party surveillance. This suggests that the primary mischief the legislature was concerned with was third party and not participant monitoring. In the present case, it would be artificial to say that Rabane was 'eavesdropping on his own conversation with the accused or that because he had a tape recorder on him he became an eavesdropper. (See the observations to similar effect of Harlan J, on behalf of the Court, in *Lopez v US* (above) 10 L Ed 2d 462 at 470.)
> Support for this approach may be derived from the terms of section 2(1)(b) itself. The statutory formulation, 'monitor a conversation', suggests that what is prohibited is the conduct of a third person acting in relation to a conversation between others. The reasoning in *S v Weinberg* 1979 (3) SA 89 (A) springs to mind. The accused had been forbidden by notice to 'attend ... any gathering'. Trollip JA, in a close linguistic construction of the banning notice, held that its

---

34 1999 (1) SACR 338 (W).

35 On page 344 *et seq.*

prohibition related to a third person attending a gathering of two others (at 104G - 105F). The terms of the banning order therefore did not prevent the banned person from herself being part of the two-person gathering.

Weinberg seems to me to provide a powerful parallel to the present case. In both, a prohibition is imposed on conduct in relation to activity (a gathering; a conversation) that in its most natural signification already involves at least two others. The prohibition must therefore be understood as relating to a third person intervening in or adding his or her presence to an already-existing two-person activity. If I am correct in this, Section 2(1)(b) of the 1992 statute must be read as applying only to third party monitoring.

The distinction I have applied to the 1992 statute has been rejected by the Supreme Court of Canada. In *R v Duarte*, La Forest J, on behalf of six members of the Court, was 'unable to see any logic to this distinction between third party electronic surveillance and participative surveillance' (65 DLR (4th) 240 (SCC) at 252g). Our Constitutional Court has yet to rule on the question. In my respectful view, notwithstanding the great respect our Constitutional Court has accorded to the decisions of the Supreme Court of Canada, that court's refusal to accept the distinction between participant and third party surveillance for constitutional purposes, is open to question.

12.2.5.28 Judge Cameron pointed out, however, that the judgment in the *Duarte* did not escape criticism:

The Canadian Court's approach is in my view correctly criticised by Peter Hogg, *The Constitutional Law of Canada,* Vol. 2, pages 45 - 12 to 45 -13, section 45.5(b). Hogg's analysis is worth quoting somewhat fully. He points out:

> In any conversation, no matter how confidential its subject matter, each participant runs the risk that his interlocutor will betray the confidence by repeating the conversation to someone else. If a participant is charged with a crime and the conversation is relevant to the charge, then his interlocutor is free to talk to the police and to testify in court about the conversation. Indeed, the interlocutor can be compelled to testify about the conversation in court. Since the disclosure of a private conversation is admissible in a court of law, then surely the recording of a conversation by a participant ought to be admissible too. The recording simply improves the participant's power of recollection making the evidence more reliable. For this reason, the Supreme court of the United States of America has held that participant surveillance is not a search and seizure within the fourth amendment. When the accused discloses the confidence to someone else, he assumes the risk that his interlocutor will reveal the confidence to the police and therefore there is no breach of a reasonable expectation of privacy when the interlocutor does reveal that confidence to the police, even when electronic aid is employed. By rejecting this distinction, the Supreme Court of Canada has produced an ironic result. The police informers in *Duarte* and *Wiggins* are free to testify in Court about their conversations with the accuseds (sic), where their memory and credibility will no doubt be challenged by the accused; but the electronic records of the conversations, which would set all doubts at rest, are inadmissible.

I interpose to observe that Hogg's contention that since first-hand evidence of the private conversation is clearly admissible, a recording of it should by corollary also be admissible is not, in my respectful view, wholly cogent. Circumstances in which a first-hand recollection of something seen or heard is admissible whereas an electronic or photographic record of what is seen or heard may not be admissible may be readily suggested. It may for example be that a person with some distinguishing feature upon his or her body may consent to another seeing it within an intimate relationship. If a camera were to be secreted upon that person and a photograph taken of the distinguishing feature, there can, in my view, be little doubt that the admissibility of the photograph could be disputed whereas the person's personal recollection can

not.

12.2.5.29 Judge Cameron further remarked that he considers Hogg's approach compelling where he argues as follows:

> In the participant surveillance cases it is not the listening in to the accused's statement that constitutes the invasion of privacy because the police agent hears only what the accused voluntarily chooses to tell him. Nor that the disclosure of the accused's statement to the police or a court, because the court in *Duarte* made clear that the police agent was free to disclose what he had heard or experienced. Therefore the invasion of privacy must consist in the electronic recording or transmitting of the statement that the accused made to the police agent. If this is so, then there would be an invasion of privacy even if the electronic record was in fact not tendered in evidence.

12.2.5.30 Judge Cameron then stated that assuming, as he does, that the distinction is sound and that section 2(1)(b) requires its application, there remains the problem of giving a meaning to section 2(2)(c):

> If a reasonable construction not impinging upon the conclusion I have just reached can be assigned to this provision, the canons of penal interpretation require me to adopt it. In my view there is such a construction. It is to be found in section 3(2), which specifies that only police, defence and intelligence officials may apply for authorisation for monitoring a conversation. That authorisation may be given not only for conversations 'by' a person, but for conversations 'with' a person (section 2(2)(c)). This seems to me to indicate that when members of the police, defence or intelligence services wish to monitor a conversation, even one 'with' a person - that is, even participant monitoring - they must obtain authorisation. The statute provides that they may obtain such authorisation from a Judge only in cases involving 'serious offences and security considerations (section 3(1)(b)(i) and (ii)). None of this applies to or concerns members of the public, whom section 2(1)(b) prohibits from engaging in third party monitoring. They are not empowered under any circumstances to seek exemption from the criminal prohibition because the monitoring they are most likely to engage in, namely participant monitoring, is not prohibited at all.
>
> The question is whether Rabane was acting as a police agent so as to fall within the prohibition of police, defence and intelligence agency participant monitoring. Rabane has testified, ... that he himself came up with the suggestion that a conversation between him and the accused be recorded. He apparently wished to authenticate the seemingly improbable story he had told the police. Mr Nel has submitted that this means that Rabane was acting privately and that the legitimacy of the recording should be judged on that basis. I have tried to approach this submission with careful scepticism. The police and other agencies should not be encouraged to circumvent statutory prohibitions with flimsy re-arrangements of personnel and operators. The events surrounding the conversation between the accused and Rabane certainly bore the hallmarks of a police operation. Even if the operation was not initiated by the police, the crucial equipment was supplied by them; they permitted Rabane to operate while he was under their supervision; they indeed directed him in how to go about the operation; and immediately after it was performed they retrieved the monitoring device and the recording from him.
>
> The source of the suggestion thus seems to me to make no decisive difference to the fact that Rabane was, broadly, acting as part of a police operation, and that he may roughly but fairly be described as having been on a 'police mission' when with the tape recorder in his pocket he approached the accused and conversed with her. Does this mean that the statutory prohibition reached him? In my view, it does not. It is true that the investigating officer could have sought

(though he could not have obtained) a Judge's direction. But Rabane himself could not have. And in the common cause circumstances before me he had good, private, reasons of his own for wanting to record the conversation with the accused. This was to establish her role in a murder in which he was damningly implicated.
The courts will no doubt be astute not to lend themselves to police stratagems to outflank the statute's prohibition. The present case does not however seem to me to involve stratagem, but a reasonable decision on the part of the investigating officer to utilize a civilian, who had a legitimate interest of his own, to record a two-party conversation. The statute did therefore not prohibit the monitoring.

12.2.5.31 Judge Cameron then considered that there may well be other reasons in the *Kidson* case for concluding that the Interception and Monitoring Prohibition Act did not apply:

The statute prohibits intentional monitoring 'so as to gather confidential information". The question is: what is confidential information'? In *Protea Technology*, Heher J pointed out that the statute does not define the term. Noting (at 603*h*) the distinction between 'confidential' and 'private' information, he suggested that the former 'must surely mean such information as the communicator does not intend to disclose to any person other than the person to whom he is speaking and any other person to whom the disclosure of such information is necessarily or impliedly intended to be restricted' (at 603g-h). This formulation seems to make the question whether the information enjoys the protection of the statutory prohibition depend largely on the intention of the communicator. I respectfully consider that it may therefore be over-broad. The statute uses a technical term, employed technically by lawyers. To my mind it is appropriate, especially in view of the fact that the statute should be interpreted narrowly, to accord the term its technical signification. To Heher J's formulation should in my view therefore be added that the information the communicator intended to restrict as confidential must be information upon which the law confers the attribute of confidentiality.
...
It therefore seems to me that information voluntarily imparted in a two-party conversation concerning the criminal conduct of the communicator is not for the purposes of the 1992 statute 'confidential information' in relation to the other party to the conversation, and therefore that participant monitoring under these circumstances is not prohibited.
...
To summarise my findings thus far:
(a) The principle of interpretation *in favorem libertatis* obliges the conclusion that the prohibition in section 2(1)(b) of the 1992 statute applies in the first instance only to third party monitoring of conversations. Its primary signification is not to cover participant monitoring, ie when one of the parties to the conversation monitors it.
(b) Police, defence and intelligence agency personnel who wish to monitor conversations for the purpose the statute specifies must however in terms of sections 2(2) and 3 obtain authorisation even for participant monitoring.
(c) A private individual who with the assistance of the police engages in participant monitoring is in the absence of proof that the operation is a sham designed to evade the statutory prohibition not covered by the criminal prohibition.

12.2.5.32 Judge Cameron also considered whether the admissibility of the recording could be attacked on constitutional grounds:

If the 1992 statute, despite my conclusion above, was applicable, it follows that there are two bases on which the accused is entitled to challenge the admissibility of the tape recording and its transcript. The first is the violation of her right to privacy in terms of section 14. The second is

that the evidence was obtained in breach of a statutory prohibition.

...

The accused, on the evidence before me, was in conversation with someone who was at best for the argument on privacy her friend, and at worst a gambling acquaintance. Her interlocutor was not her spouse or life partner. She was not in any counselling or therapeutic relationship with him. She was not receiving ministration or psychological or pastoral or religious support from him. There was no legal or contractual relationship between them. He was not even on the evidence so far before me a close friend. On these facts it is impossible, in my view, to find there are any discernible privacy interest was violated when Rabane recorded and published the conversation between them. The point is made with telling effect by Hogg (above) where, ... he goes on to criticise what he terms the Supreme Court of Canada's 'extravagant notion of privacy' (page 45-13), section 45.5(b)). In my view the argument for the accused here likewise relies upon an inappropriately extravagant notion of privacy. The accused chose to share her recollections and reflections with Rabane, and by doing so she accepted the risk that he might impart them to someone else. ...

I therefore rule that no constitutionally cognizable breach of privacy occurred when the police procured the monitoring by the suspect Rabane of his conversation with the accused.

That, however, is not the end of the matter. On the assumption I have made the statute was breached when Rabane approached the accused without the police having obtained prior judicial authority for the monitoring in question. ...

The extent and flagrancy of the statutory contravention remains an issue to be weighed by the court in exercising its discretion as to whether to admit the evidence or not.

...

Despite my assumption in favour of the accused that the statute was applicable and that it was breached, it seems to me that the extent of the police violation was here minimal.

12.2.5.33 The Commission also notes the following succinct remarks by La Forest J[36] of the Canadian Supreme Court in the case of *R v Wong*[37] which clearly deals with unauthorised video surveillance but carefully analyses the role of government agencies in a free and open society:

> I am firmly of the view that if a free and open society cannot brook the prospect that the agents of the state should, in the absence of judicial authorization, enjoy the right to record the words of whomever they choose, it is equally inconceivable that the state should have unrestricted discretion to target whomever it wishes for surreptitious video surveillance. George Orwell in his classic dystopian novel 1984 paints a grim picture of a society whose citizens had every reason to expect that their every movement was subject to electronic video surveillance. The contrast with the expectations of privacy in a free society such as our own could not be more striking. The notion that the agencies of the state should be at liberty to train hidden cameras on members of society wherever and whenever they wish is fundamentally irreconcilable with what we perceive to be acceptable behaviour on the part of government. As in the case of audio surveillance, to permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society. There are, as *R. v. Dyment*, [1988] 2 S.C.R. 417, at pp. 428-29, tells us, situations and places which invite special sensitivity to the need for human privacy. Moreover, as Duarte indicates, we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy.

---

36 The judgment of Dickson C.J. and La Forest, L'Heureux-Dubéé and Sopinka JJ. was delivered by La Forest J.

37 [1990] 3 SCR 36.

R. v. Duarte was predicated on the notion that there exists a crucial distinction between exposing ourselves to the risk that others will overhear our words, and the much more pernicious risk that a permanent electronic recording will be made of our words at the sole discretion of the state. Transposing to the technology in question here, it must follow that there is an important difference between the risk that our activities may be observed by other persons, and the risk that agents of the state, in the absence of prior authorization, will permanently record those activities on videotape, a distinction that may in certain circumstances have constitutional implications. To fail to recognize this distinction is to blind oneself to the fact that the threat to privacy inherent in subjecting ourselves to the ordinary observations of others pales by comparison with the threat to privacy posed by allowing the state to make permanent electronic records of our words or activities. It is thus an important factor in considering whether there has been a breach of a reasonable expectation of privacy in given circumstances.

The Applicability of s. 8 of the Charter on the Facts of this Case

I turn from these general observations to the question whether, on the facts of this case, the appellant could be said to have had a reasonable expectation of privacy. The Court of Appeal, after stating, by way of an initial premise, that a person attending a function to which the general public has received an open invitation can have no interest in "being left alone", went on to draw the following conclusions from the facts of this case, at p. 373:

> None of the respondents testified that they had a subjective expectation of privacy and it is difficult to believe that they could give such evidence. It may well be that they were in the same room with strangers. The occupants' only common interest was to gamble illegally for high stakes. All but Santiago Wong were no more than casual visitors to the rooms with no basis for challenging the legality of the search. Neither is it possible that Santiago Wong had any reasonable expectation of privacy. He was booking the room regularly and it was clear from police observation that the room had been used for gambling on other occasions. Wong had invited and accepted so many people into the room that there could not have been any reasonable expectation of privacy by anyone in the room, least of all Santiago Wong who benefited by the presence of the others.
>
> Video surveillance of persons in a hotel room could in certain circumstances constitute a search of the most intrusive kind. However, in this case, as there was no reasonable expectation of privacy, s. 8 of the Charter cannot have any application.

I think, with respect, that the conclusions of the Court of Appeal cannot be reconciled with the implications of this Court's subsequent decision in *R. v. Duarte*. The Court of Appeal has, in effect, applied a variant of the risk analysis rejected by this Court in that case, for it has chosen to rest its conclusion on the notion that the appellant, by courting observation by the other persons in the room, has effectively relinquished any right to maintain a reasonable expectation of freedom from the much more intrusive invasion of privacy constituted by surreptitious video surveillance on the part of the state.

Moreover, it is clear from the excerpt cited above that the Court of Appeal, in assessing the constitutionality of the search, has allowed itself to be influenced by the fact that the appellant was carrying on illegal activities. By way of expansion on my earlier references to *Duarte*, I would note that that decision places considerable emphasis on the fact that the answer to the question whether persons who were the object of an electronic search had a reasonable expectation of privacy cannot be made to depend on whether or not those persons were engaged in illegal activities; see pp. 51-52. If reliance were to be placed on such ex post facto reasoning, and the courts to conclude that persons who were the subject of an electronic search could not have had a reasonable expectation of privacy because the search revealed that they were in fact performing a criminal act, the result would inevitably be to adopt a system of subsequent validation for searches. Yet it was precisely to guard against this possibility that this Court in *Hunter v. Southam Inc.*, supra, at p. 160, stressed that prior authorization, wherever feasible, was a necessary pre-condition for a valid search and seizure. As noted in *R. v. Dyment*, supra, at p. 430, this is inherent in the notion of being secure against unreasonable searches and seizures.

Accordingly, it follows logically from what was held in *R. v. Duarte* that it would be an error to suppose that the question that must be asked in these circumstances is whether persons who engage in illegal activity behind the locked door of a hotel room have a reasonable expectation of privacy. Rather, the question must be framed in broad and neutral terms so as to become whether in a society such as ours persons who retire to a hotel room and close the door behind them have a reasonable expectation of privacy.

Viewed in this light, it becomes obvious that the protections of s. 8 of the Charter are meant to shield us from warrantless video surveillance when we occupy hotel rooms. Clearly, our homes are places in which we will be entitled, in virtually all conceivable circumstances, to affirm that unauthorized video surveillance by the state encroaches on a reasonable expectation of privacy. It would be passing strange if the situation should be any different in hotel or motel rooms. Normally, the very reason we rent such rooms is to obtain a private enclave where we may conduct our activities free of uninvited scrutiny. Accordingly, I can see no conceivable reason why we should be shorn of our right to be secure from unreasonable searches in these locations which may be aptly considered to be our homes away from home. Moreover, *R. v. Duarte* reminds us that unless the question posed in the preceding paragraph is answered in neutral terms as I have suggested, it follows not only that those who engage in illegal activity in their hotel rooms must bear the risk of warrantless video surveillance, but also that all members of society when renting rooms must be prepared to court the risk that agents of the state may choose, at their sole discretion, to subject them to surreptitious surveillance; see again at pp. 51-52.

Nor, with respect, can I attach any importance to the fact that in the circumstances of this case the appellant may have opened his door to strangers, or circulated invitations to the gaming sessions. I am simply unable to discern any logical nexus between these factors, and the conclusion that the police should have been free to videotape the proceedings in the hotel room at their sole discretion. It is safe to presume that a multitude of functions open to invited persons are held every week in hotel rooms across the country. These meetings will attract persons who share a common interest but who will often be strangers to each other. Clearly, persons who attend such meetings cannot expect their presence to go unnoticed by those in attendance. But, by the same token, it is no part of the reasonable expectations of those who hold or attend such gatherings that as a price of doing so they must tacitly consent to allowing agents of the state unfettered discretion to make a permanent electronic recording of the proceedings.

We must be prepared to live with the first risk, but, in a free and open society, need not tolerate the spectre of the second. As I have intimated above, this seminal distinction between what is constitutionally acceptable and unacceptable follows inexorably from the point made in *R. v. Duarte* that it would be an error to equate the risk of having one's words overheard with the risk of having the state, at its sole discretion, make a permanent electronic recording of those words. At p. 48 of that decision, it was said that these threats to privacy are of a different order of magnitude and involve different risks to the individual and the body public. The same must be true of the risk of being the object of private scrutiny, and the risk of having a permanent electronic recording made of one's presence in a given location at the behest of the state.

I therefore conclude that the Court of Appeal erred when it held that the appellant did not have a reasonable expectation of privacy in the circumstances of this case. Were the reasonableness of unauthorized video surveillance to be gauged by the standard adopted by the Court of Appeal the state would be at liberty to train its hidden cameras on an extremely broad spectrum of the activities engaged in by members of society. In effect, we would be debarred from asserting a reasonable expectation of freedom from clandestine electronic scrutiny on the part of the state at any private function to which members of the public had received an invitation.

Moreover, it is also clear that those ordinary measures which persons in a free and open society believe suffice to shut out uninvited scrutiny would be of no avail if the police (and they would of course be the sole arbiters of the matter) entertained the suspicion that the persons in the location concerned were involved in illegal activity. Here, it must be remembered that while the appellant had rented a room in an establishment to which selected members of the public had access, he had seen to it that activities in the room were conducted behind locked doors and drawn drapes.

> In effect, by application of the standard adopted by the Court of Appeal, members of society would be driven back to the confines of their homes if they wished to be sure of being able to escape the risk of unauthorized video surveillance. And even this ultimate refuge could be breached if the police formulated a suspicion with respect to gatherings in the home, for I think it must be conceded that on the reasoning of the Court of Appeal the appellant could have asserted no reasonable expectation of privacy if the gambling sessions had been conducted in his own home.
>
> By way of recapitulation on this important point, I think it can be seen that the approach taken by the Court of Appeal to the question of what constitutes a reasonable expectation of privacy simply cannot be reconciled with the conclusions that emerge from *R. v. Duarte*. That decision makes it clear that s. 8 of the Charter is meant to protect those expectations on which we rest our belief that our society is one in which we are not exposed to unauthorized clandestine electronic surveillance on the part of the state. I take it to be beyond dispute that just as we hold to the belief that a free and open society is one in which the state is not free to make unauthorized recordings of our conversations, so too it is no less an article of faith in a society that sets a premium on being left alone that its members presume that they are at liberty to go about their daily business without courting the risk that agents of the state will be surreptitiously filming their every movement. By simple analogy with *R. v. Duarte*, it must follow that unauthorized video surveillance will be found to offend against the reasonable expectations of privacy protected by s. 8 in the circumstances here. Certainly it is inconceivable to me that the police should enjoy the latitude to make surreptitious video recordings that is implicit in the conclusions of the Court of Appeal.

12.2.5.34 The Commission considers that another aspect to be taken into account is the accused's right to silence and against self-incrimination. The Canadian Supreme Court gave the following insightful exposition of this aspect in the case of *R v Broyles*[38]:

> In every case where the right to silence is raised, the threshold question will be: was the person who allegedly subverted the right to silence an agent of the state? In answering this question one should remember that the purpose of the right to silence is to limit the use of the coercive power of the state to force an individual to incriminate himself or herself; it is not to prevent individuals from incriminating themselves *per se*. Accordingly, if the person to whom the impugned remarks is made is not an agent of the state, there will be no violation of the right to silence.
>
> In some cases, it will be clear that the person to whom the statements were made was an agent of the state. For example, if the statements were made to a police officer or to a prison official, whether in uniform or in plainclothes, there could be no question that the statements were made to an agent of the state. In other cases, it will be less clear. Where the statements are made to an informer, as in the case at bar, it may be arguable whether or not the coercive power of the state was brought to bear on the suspect in obtaining the statement from him or her.
>
> In determining whether or not the informer is a state agent, it is appropriate to focus on the effect of the relationship between the informer and the authorities on the particular exchange or contact with the accused. A relationship between the informer and the state is relevant for the purposes of s. 7 only if it affects the circumstances surrounding the making of the impugned statement. A relationship between the informer and the authorities which develops after the statement is made, or which in no way affects the exchange between the informer and the accused, will not make the informer a state agent for the purposes of the exchange in question. Only if the relationship between the informer and the state is such that the exchange between the informer and the accused is materially different from what it would have been had there been no such relationship should the informer be considered a state agent for the purposes of the

38 [1991] 3 S.C.R. 595.

exchange. I would accordingly adopt the following simple test: would the exchange between the accused and the informer have taken place, in the form and manner in which it did take place, but for the intervention of the state or its agents?

If this test is applied to a conversation between a police officer and a suspect in custody, it is clear that the conversation would not have taken place but for the intervention of the officer. If it is applied to a conversation with a cell mate who has no contact with the authorities until after the conversation is concluded, it is equally clear that the actions of the authorities had no effect on the conversation, and that there would be no violation of the s. 7 right to silence. If, however, the cell mate spoke with the authorities before the conversation took place, then the question will be whether the conversation would have occurred or would have taken the same course had the cell mate had no contact with the authorities.

I would add that there may be circumstances in which the authorities encourage informers to elicit statements without there being a pre-existing relationship between the authorities and individual informers. For example, the authorities may provide an incentive for the elicitation of incriminating statements by making it known that they will pay for such information or that they will charge the informer with a less serious offence. The question in such cases will be the same: would the exchange between the informer and the accused have taken place but for the inducements of the authorities?

(b) *Elicitation*

Even if the evidence in question was acquired by an agent of the state, it will only have been acquired in violation of s. 7 if the manner in which it was acquired infringed the suspect's right to choose to remain silent. In general, there will be no violation of the suspect's right to silence if the suspect volunteers the information, knowing he or she is talking to an agent of the state. In the words of McLachlin J. in *Hebert*, *supra*, at p. 184:

> If the police are not posing as undercover officers and the accused chooses to volunteer information, there will be no violation of the *Charter*. Police persuasion, short of denying the suspect the right to choose or depriving him of an operating mind, does not breach the right to silence.

In *Hebert*, *supra*, my colleague McLachlin J., left open the possibility that there will be cases amounting to more than permissible police persuasion but less than deprivation of an operating mind which will infringe the suspect's right to choose to remain silent. I would agree that there may well be such cases, but it is unnecessary to decide that question in this case.

If, on the other hand, the suspect is ignorant of the fact that he is talking to an agent of the state, whether a suborned informer or an undercover police officer, somewhat different considerations will apply. It is clear from the majority reasons in *Hebert*, *supra*, that statements volunteered by the suspect to the agent of the state will not infringe the suspect's right to silence. There will be a violation of the s. 7 right to silence only if the statement is elicited by the agent of the state. As McLachlin J. expressed it in *Hebert*, *supra*, at p. 184, the state agent must "actively elicit" the information or statement. The focus will be on what constitutes "elicitation" in the context of the right to silence.

In developing a definition of elicitation, I have found it unnecessary to refer at length to the U.S. jurisprudence dealing with the Fifth and Sixth Amendments of the U.S. Constitution. In broad terms, the concern with Sixth Amendment right to counsel is, to quote the judgment of Brennan J. in *Maine v. Moulton*, 474 U.S. 159 (1985), at p. 176, to protect the right of an accused "to rely on counsel as a `medium' between him and the State," and not specifically to protect the right of an accused to choose whether or not to make a statement. Although the Fifth Amendment privilege against self-incrimination is similar in form to the right to silence in s. 7 of the *Charter*, the Supreme Court of the United States has recently held, in *Illinois v. Perkins*, 110 S.Ct. 2394 (1990), that Fifth Amendment rights do not prohibit surreptitious jail house conversations of the kind which this Court found to violate s. 7 in *Hebert*. This is not to say that the U.S. jurisprudence will not be useful in resolving particular problems that may arise in developing the contours of the right to silence as McLachlin J. did in *Hebert*. In general, however, Canadian courts should not be hesitant to develop a uniquely Canadian approach to the right to silence, in keeping with the overall goals of the *Charter*.

In my view, it is difficult to give a short and precise meaning of elicitation but rather one should

look to a series of factors to decide the issue. These factors test the relationship between the state agent and the accused so as to answer this question: considering all the circumstances of the exchange between the accused and the state agent, is there a causal link between the conduct of the state agent and the making of the statement by the accused? For convenience, I arrange these factors into two groups. This list of factors is not exhaustive, nor will the answer to any one question necessarily be dispositive.

The first set of factors concerns the nature of the exchange between the accused and the state agent. Did the state agent actively seek out information such that the exchange could be characterized as akin to an interrogation, or did he or she conduct his or her part of the conversation as someone in the role the accused believed the informer to be playing would ordinarily have done? The focus should not be on the form of the conversation, but rather on whether the relevant parts of the conversation were the functional equivalent of an interrogation.

The second set of factors concerns the nature of the relationship between the state agent and the accused. Did the state agent exploit any special characteristics of the relationship to extract the statement? Was there a relationship of trust between the state agent and the accused? Was the accused obligated or vulnerable to the state agent? Did the state agent manipulate the accused to bring about a mental state in which the accused was more likely to talk?

In considering whether the statement in question was elicited, evidence of the instructions given to the state agent for the conduct of the conversation may be important. As McLachlin J. noted in *Hebert, supra*, evidence that the agent was instructed not to initiate the conversation nor to ask leading questions will tend to refute the allegation that the resulting statement was obtained in violation of s. 7. I would add, however, that in my opinion evidence that the state agent was instructed not to elicit information will not end the inquiry. The authorities may not take the benefit of the actions of their agent which exceed his or her instructions. To hold otherwise would be to ignore the fact that the primary emphasis of the right to silence in s. 7 is on the use of the coercive power of the state against the suspect. The authorities ought not to be able to shield themselves behind the subtleties of their relationship with the informer. It is the authorities who are in a position to control the actions of their informer; if they fail to do so, they ought not to benefit from that failure at the expense of the accused. See *United States v. Henry*, 447 U.S. 264 (1980), at pp. 271-72.

(c) *Application to the Facts of This Case*

There is no question that Ritter was an agent of the state during his conversation with the appellant. It is clear on the evidence that the meeting was set up and facilitated by the police. Ritter was able to have an "open visit" with the appellant, which made possible a free-ranging conversation, only because of the intervention of the police. In fact, Ritter went so far as to admit that he was not frightened during his visit with the appellant "because it had been set up by the police". Moreover, in their discussions with Ritter, the authorities effectively instructed him to elicit information about the death of Briggs ...

12.2.5.3.35 The Commission has carefully considered the points of view expressed in the *Duarte*, *Wong, Broyles* and *Kidson* cases on the role of law enforcement agencies. It has also taken into account the opposing suggestions made by respondents such as Judge Gordon and the SA Police Service who argue, on the one hand that the law enforcement agencies should be allowed in participant monitoring circumstances to intercept and record conversations without obtaining a directive first and those respondents who argue, on the other hand, that directives should be obtained under these circumstances since the consent of one of the participant to the conversation is not sufficient. The Commission considers that the reasoning by Judge Cameron in the *Kidson* case is persuasive and that where police, defence and

intelligence agency personnel wish to monitor conversations for the purpose the statute specifies, they must in terms of sections 2(2) and 3 obtain authorisation even for participant monitoring. The Commission is of the view that the project committee's proposed clause does not solve the issue satisfactorily. The Commission considers that section 2 should make it further clear that members of the South African Police Service, the South African National Defence Force, the Agency and the Service may only intercept or monitor a conversation or communication if a directive is issued by a judge in terms of the Act to authorise such interception or monitoring.

(c) Recommendation

12.2.5.36 The Commission recommends that it be made further clear in section 2 that save as is provided in section 3 no person shall intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications system or intentionally monitor any communication by means of a monitoring device so as to gather confidential information concerning any person, body or organization.

12.2.6 Clause 3(1)(a): designation of judges

(a) Comments on clause 3(1)(a)

12.2.6.1 The Office of the Director Investigating Directorate Organised Crime and Public Safety and the submission forwarded by the Director Public Prosecution of Cape of Good Hope comments as follows:

> Dit word aanbeveel dat alle regters, uitsluitende waarnemende regters, aangestel word vir doeleindes van hierdie Wet. Alternatiewelik beveel respondent aan dat elke Provinsiale en Plaaslike afdeling sy eie Regter kry wat vir doeleindes van hierdie wet aangestel word. Daar word egter aanbeveel dat die betrokke aangewese Regter of die Regter President van elke plaaslike afdeling die reg van substitusie sal hê. Ondervinding het geleer dat Regters vir verskeie redes nie beskikbaar is om met aansoeke in gevolge hierdie wet te handel nie met die gevolg dat belangrike inligting verlore gaan en/of dat inligting wederregtelik bekom word wat dan weer verdere bewysregtelike probleme skep. Wat in die praktyk geleer is, is dat waar daar dringende aansoeke en/of verlengingsaansoeke is en die Regter aangewys ingevolge hierdie wet nie beskikbaar is nie dit meer raadsaam is om iemand te hê wat hom op kort kennisgewing kan vervang as om die betrokke aansoek en/of verlening te laat skipbreuk

lei.

Praktiese ondervinding het geleer dat indien daar nie 'n regter vir elke afdeling is me, maar soos huidiglik slegs een regter te Pretoria gesetel is en aansoeke vanaf Kaapstad byvoorbeeld gestuur word, daar verskeie administatiewe en logistieke probleme kan ontstaan.

Daar word aanbeveel dat daar nie onderskeid gemaak word tussen Nasionale Intelligensie en emstige misdrywe nie. Die rede hiervoor is dat die praktyk geleer het dat wanneer die nood druk daar gegryp word na alle beskikbare inligting. Sou daar dan een sentrale Regter wees wat slegs nasionale inligting aangeleenthede hanteer en waar hy in Pretoria gesetel sal wees, sal dit beteken dat hy nie vir die betrokke plaaslike of provinsiale afdeling aangewys is om monitoring te magtig nie. Dit het dan ook in die verlede gebeur dat 'n monitering gedoen word met die oog daarop om dit nie in kriminele aangeleenthede te gebruik nie. Waar daar dan egter 'n noodsituasie ontstaan en alle meganismes om misdaad te bekamp is uitgeput dan word daar na hierdie inligting gegryp. Die frustrasies is dan baie hoog waar hierdie inligting wat in baie gevalle goeie inligting is en goeie getuienis sal wees in 'n kriminele saak nie in'n kriminele saak aangebied kan word nie as gevolg van bewysregtelike probleme wat ontstaan. Respondent beveel dus aan dat die regters wat aangewys word in elke provinsiale en plaaslike afdeling ook nasionale inteligensie aansoeke moet hanteer en dat daar aan dieselfde voorskrifte en vereistes voldoen word as vir ernstige misdrywe.

12.2.6.2 Ms Naicker[39] comments that the dual system of judges as is common in most European countries may be suitable for the South African situation. She considers that the dual system of judges should consist of a panel of judges whose main function would be to consider applications by the National Intelligence Agency (NIA), South African National Defence Force (SANDF), South African Police Services (SAPS) and the South African Secret Service (SASS). She states that these applications should be restricted to matters that affect security of the country, international relations and other matters of national interest. She considers that the second part of the system should consist of the appointment of a judge in each Provincial Division that shall be designated to consider applications that relate to the interception and monitoring during ordinary criminal investigations. She notes that the system may have a financial implication in that more judges would have to be appointed but the corollary is that the system will operate more efficiently. Ms Naicker remarks that the additional judges would assist in relieving the current backlog of cases that exists in our judicial system.

12.2.6.3 Ms Naicker considers that the judges need not only deal with applications in terms of the Act. She notes that the additional judges will also assist in the crime prevention

39 Of the Department of Public Works.

programme, as the investigators would not have to follow the usual judicial process to make an application in terms of the Act and that these judges shall deal with the applications.

12.2.6.4 M-Web considers that whilst the Discussion Paper reflects a commitment to a "judicial model" for the issuing of an authority to monitor and intercept, the concern that they have is the extent to which designating particular judges to perform this task - either nationally or in a particular division - may establish a relationship that becomes routine. M-Web points out that it is not their intention to question judicial independence but given that the proposed legislation envisages grave inroads into fundamental rights it may be preferable that the authorities apply for a warrant from a judge in the ordinary course, subject to such "in camera" requirements as may be reasonably be imposed in the circumstances. M-Web states that in this way a fresh mind is brought to bear on each occasion that an authority is sought. M-Web remarks that they are also concerned that there is an absence of due process rules, apart from those that may or may not be applicable in terms of the Constitutional Act No. 108 of 1996, in much of the activities undertaken by the Minister.

12.2.6.5 The SAPS[40] notes that there is a strong feeling from the South African Police Service in some provinces that judges should be appointed in the respective divisions to deal with crime related applications for interception and monitoring. They note that it is expected that, if the proposed amendments of the Act are approved, that there will be a sharp increase in applications for interception and monitoring. The SAPS considers that a panel of judges (the option favoured by the Commission) will not provide a bigger capacity than a single judge. The SAPS states that it is not necessary to appoint a judge in respect of each Division, but that a number of say 4 judges could be appointed in respect of the whole country or certain regions. The SAPS considers that this will greatly enhance the capacity to deal with applications. The SAPS considers that the following aspects should be kept in mind:

(a) Security
Vetting of personnel, physical and communications security measures will have to be taken in respect of each judge designated to consider applications.

(b) Preferences of the service providers
The service providers prefer that the original directions be submitted at a central point to them for execution and they are geared to handle the execution in that way. This aspect could, however, be renegotiated.

---

40 Chief Manager: Legal Component Detective Sevices.

12.2.6.6 The SAPS states that another possibility, which is officially preferred by the South African Police Service, could be to designate a number of judges, say 3 in respect of the whole country, but have them situated in one central office in Pretoria. They note that it is, however, appreciated that the designation of judges, their offices etc. is a matter primarily concerning the Department of Justice and the opinion of that Department in this regard will be important.

12.2.6.7 The NICOC subcommittee states that it supports the idea of one cetralised office, at least as far as security-related matters are concerned. They remark that they do not support the idea of a panel of judges dealing with applications as a panel. They consider that it is, however, advisable to designate at least one other judge to stand in for the designated judge when he or she is not available (eg on leave). The NICOC subcommittee points out that they are not entirely opposed to the designation of judges in the provinces, provided that financial, security, and practical considerations are accounted for, and provided that applications for, or the execution of, directives given by these judges should not be limited to their areas of jurisdiction. They propose that a new subsection 7 be considered to cater for amendments to an existing directive, such as:

> (1) The judge referred to in subsection (1) may, upon an application that complies with the directives referred to in section 6, direct further additions or amendments to an existing direction referred to in section 2(2) if the judge is satisfied that the addition or amendment is necessary for a reason referred to in subsection (1)(b)(i) or (ii).

12.2.6.8 The Cape Law Society's Criminal Law and Procedure Committee remarks that the committee strongly recommends that it be required that applications for the issue of warrants be heard by more than one judge to ensure that process by which such warrants are issued is as objective as possible.

12.2.6.9 The National Intelligence Agency[41] comments that they have noted that the Minister will be able to designate one judge for all court divisions to hear all security related applications. They agree with this approach.

12.2.6.10 The SAPS[42] comments that they support a panel of review but not a panel for

---

41 Deputy Director-general Operational Services .

42 Office of the Commander Technical Support Unit Eastern Cape.

consideration. They state that the reason is that it will be difficult to urgently convene a panel of judges therefore a panel of judges would be suited for review a time convenient for all concerned.

12.2.6.11 Judge Gordon[43] states that this is probably one of the most important matters dealt with in the discussion paper, i. e. recommending a fundamental change to the body constituted to deal with applications, and deserves full consideration. He recommends that a dual system be employed as in most European countries. He says he could add that the United States of America has a form of dual system constituted by the Foreign Intelligence Surveillance Act. Judge Gordon explains that the U. S.A. Chief Justice designates seven district court judges from seven judicial circuits to hear applications and elaborate procedures are provided with detailed jurisdictional powers relating *inter alia* to the nature of the matters to be dealt with, corresponding broadly to what is proposed in the paper, namely applications emanating from NIA, SASS and SANDF. Matters dealt with under FISA may include matters of ordinary crime. Judge Gordon notes that in Great Britain the Home Office and the National Criminal Intelligence Service (NCIS) have departments dealing separately with persons (bodies) whose activities pose a threat to the interests of the United Kingdom. He notes that a "dual system" even where functions may on occasions merge, is thus acceptable in most systems of surveillance.

12.2.6.12 Judge Gordon remarks that the reason for appointment of additional judges, constituting a dual system, would not be due to excessive volume of work. He states that he, as single judge, have managed adequately with applications country-wide, unaffected by distance. Applications are faxed through to be processed in Pretoria and dealt with at his office here. He would suggest that there may correctly be a perception that additional judges doing the work may result in improved efficiency and convenience, and this by itself would be sufficient to warrant the further appointments. In his view a decision to appoint additional judges will prevail and his comments, offered on this basis, are as follows:

3. The judge at the central office will remain here, as before, as a full-time judge. The other judges will do this duty additionally to their daily routine. An example would be as they attend to Magistrates' Courts reviews. Following upon my next comment, the judge in each region will have ample time to attend to the matters placed before him, which would probably not be on a daily basis.
4. I suggest that the establishment of three regions would be sufficient, perhaps as

---

43 Of the Office for Control of Interception and Monitoring of Communications.

a trial pilot scheme, with headquarters respectively at Cape Town, Durban and Pretoria. There would certainly be insufficient work for a judge in each province. The Minister should have the power to define regions and make the necessary adjustments to appointments on jurisdiction. A paramount consideration will be the maintenance of Top Secrecy and confidentiality. I need not elaborate. (See e.g. your discussion paper Para K, L. 99).

5. It would be essential to establish adequate security provisions with suitably qualified staff. I might suggest that a study of security arrangements in this office might be profitable and we would gladly assist.
6. The present office should be maintained as the central office for the permanent judge with sole authority for all applications from NIA, SASS and SADF. However, I recommend that this Judge should have concurrent jurisdiction, country-wide, to deal with any applications from the SAPS (i.e. crime-related). The SAP S would then have a choice as a matter of convenience, to submit any application to this judge. I should point out that crime-related applications from the SAPS might not necessarily be regionally territorial, especially in relation to syndicated crime. An application granted last week related to intercepts etc. in three provinces.

5 . While the full-time judge at the central office would not be a court of review or have any senior status as regards the work in other regions, he might be in a position to assist with advice or discussion if so desired by a judge doing the work part-time. This office would always be available for any assistance, especially to a newly-appointed judge.

6. The question of providing meaningful statistics to the Minister has been a matter I have discussed at length with the Units, particularly NIA and SAPS. I have made available copies of statistics prepared and maintained by the parties overseas, fully reported on in my report of my overseas trip. Much work will be entailed in doing this work and it is my recommendation that this central office be designated as the office responsible for this work. The agencies overseas consider this work indispensable to proper investigations which would, *inter alia* provide information on how successful or effective this work is in the fight against crime, the costs involved, the areas calling for improvement, consolidation, effectiveness of extensions of applications (sometimes for years) and so forth. I have spent much time on this aspect, have much documentation, and would gladly advise and assist in this connection. In my view the question of maintaining and analysing statistics properly prepared is the key to the proper functioning of Interception, Monitoring, Electrical Surveillance, etc.
7. I referred earlier to the question of preparing and distributing Rules which would relate to proper functioning of our work. The Rules would cover a wide field and should prove to be of great assistance to investigation officers (field work), the preparing and reviewing authorities and the appointed judges. The method of preparation of statistics would be included in the Rules. Consideration should be given to inserting a clause authorising the preparation of Rules by the permanent judge. The Rules would also be distributed to SAPS and that body would also be obliged to maintain the necessary statistics, to be forwarded to the central office. The judge at the central office would then be able to compile a comprehensive report with useful statistics for the Minister in the form of the report by the Commissioner for Interception in Great Britain, a printed copy whereof is available.

12.2.6.13 Vodacom notes that the level of intrusion into the privacy of an individual that can

be achieved by utilising mobile cellular technology is very high and poses a real danger of a serious violation of a person's aforementioned constitutional right. The implementation of any of the provisions of the Act should therefore be strictly based on a directive issued by a judge of the High Court of South Africa. Vodacom supports the appointment of a national panel of judges to deal with both security related and serious criminal offences in terms of the Act. Vodacom considers that this will ensure that applications will be dealt with in a uniform and consistent manner, and it will facilitate the establishment of a central record-keeping system for the effective and co-ordinated management of the implementation of the Act. Vodacom also recommends that the panel submit an semi-annual report to the Ministers of Telecommunications and Justice, and they in turn to special subcommittees of their respective Parliamentary standing committees. Vodacom states that this will serve as a system of "checks and balances", and most importantly, given the unavoidable limitations on technological and administrative capacity, it is imperative that the panel maintain a list - for each operator - indicating the priority of execution of all currently active directives. Vodacom remarks that networks cannot be expected to decide between various directives issued at various points which will inevitably end up competing for limited resources, especially given the severe penalty provisions which are proposed. Vodacom proposes the following clause:

(a) designated by the Minister of Justice
  (i) in each division to consider only applications in terms of this Act relating to serious offences; provided that
  (ii) the aforementioned judges constitute a national panel of judges which shall compile and submit a semi-annual report, reflecting the number and nature of directions granted per division, to the Ministers of Telecommunication and Justice, who shall submit it to the special sub-committees of their respective Parliamentary standing committees; and provided further that
  (iii) the Minister may designate a judge who will be a member of the panel referred to in (ii) above, for more than one division to consider only applications in terms of this act relating to the security of the Republic, and"

12.2.6.14 Mr Harold Marshall considers that to avoid the abuse of surveillance, interception and monitoring, control must be established. He suggests that the path required for permission needs to be defined and proposes the following model:

(b) A number of Judges need to be appointed throughout the country. This will ease the burden on a single Judge as well as allowing for faster processing of urgent applications by officers in the particular area. It may be worthwhile considering additional Judges to concentrate on specialised criminal activities where knowledge

of the crimes and modus operandi are familiar.

(c) An idea is that the Minister of Justice should have the authority to appoint any one to this position and not only a Judge.

(d) There are many excellent retired Police Officers who have a wealth of knowledge in legal investigation methods and the law. The Department should make use of these people and their knowledge.

(e) In my presentation at the International Crime conference last year, one of the ideas I put forward was a form of tiered responsibility. This allowed the Investigators a quicker route for applications at different levels of investigation or the use of surveillance equipment. It also maintained a check against the illegal use of surveillance equipment.

(f) After the final amendment, a training course or seminar should be held for Judges, Magistrates, Prosecutors and Investigation Officers. This will bring awareness of the laws to all concerned. If there are any grey areas that need clarification, they can be referred back to the commission and explanatory notes can be sent to all.

Judges or Magistrates will then have terms of reference to consult, without having to postpone cases for clarification.

(g) I would like to recommend that applications by registered, qualified or listed private investigators should also be considered. Due to the workload at present, the SA Police may not have the manpower to handle an investigation. At this time, many companies are using private investigators to obtain all the evidence required for a conviction. The case is only then handed to the Police and a case is opened for prosecution.

Possibly, with the approval of a Branch Commander or similar rank, an application can be made and approved for private investigators to carry out the surveillance and monitoring. Bona fide private investigation companies should apply to be on an approved list. This will help to eliminate 'fly-by-night' detectives.

12.2.6.15 Mr Marshall considers further that crimes do not have boundaries and that the person designated by the Minister should be able to issue the directive for any part of the country. He suggests that a crime may start in one division and then move to another division although the Judge has issued a directive in the area the crime started. He proposes that the investigator should be allowed to follow the crime anywhere as long as the directive covers either the person or the address or that crime activity. He suggests that at least one of the links must be continuous. Mr Marshall is of the view that to assemble a panel of Judges may not be practical to get all of them together at the same time. He considers that it will also be time consuming and may be detrimental to an investigation that requires immediate or urgent attention. Mr Marshall is of the view that when the Minister appoints the Judges or persons,

the scope of their authority can be listed. He suggests that the Minister should be able to amend their scope at any time and in this way, Judges can cover more than one aspect and different aspects can be covered by more than one Judge.

(b) Evaluation

12.2.6.16 The project committee considered that there is so much overlapping of matters involving serious crimes and state security that it would be inadvisable to try to separate them, as the prosed clause seeks to do in that a judge or judges be designated to consider only applications relating to state security. The committee resolved that subparagraph (ii) providing for the designation of judges considering applications relating to state security should be deleted. The committee also noted the practical difficulties involved in only one judge being designated to entertain all applications made in the country, such as someone from Cape Town rushing to Pretoria to him or her with an application. The committee resolves that "only" should be deleted in section 3(1)(a)(i) in the phrase "in each division to consider only applications".

12.2.6.17 The committee noted that if a police official who keeps a suspect under surveillance and perhaps follows the suspect on foot or monitors the movements of the suspect, does not need a go to a judge to get a warrant from a judge but when one is dealing with electronic surveillance, they do have do so. The committee posed the question whether the question of privacy under these circumstances are not over-exaggerated for commercial reasons.

12.2.6.18 The Commission agrees with the project committee that there is so much overlapping of matters involving serious crimes and state security that it would be inadvisable to try to separate them, and that the proposed subparagraph (ii) providing for the designation of judges considering applications relating to state security only, should be deleted. The Commission is further of the view that the project committee's proposal for the deletion of the word "only" should be deleted in section 3(1)(a)(i), is persuasive.

(c) Recommendation

12.2.6.19 The Commission recommends that provision be made for the designation of judges by the Minister of Justice to consider applications made under the Act, and that the proposed subparagraph (ii) providing for the designation of judges considering applications relating to

state security only, should be deleted. The Commission recommends further that the word "only" should be deleted in section 3(1)(a)(i).

12.2.7 Clause 3(1)(b): if the judge is satisfied on the facts alleged in a written application that there are reasonable grounds to believe that the offence committed is serious which cannot be investigated in another appropriate manner

(a) Comments on the proposed clause

12.2.7.1 It is proposed in the discussion paper that section 3 of the Monitoring Act be amended by substituting the words "where the proposed monitoring referred to in section 2(2)(c) will be carried out; and" with the phrase "to consider only applications in terms of this Act relating to the security of the Republic,".

12.2.7.2 MTN considers that this proposed amendment to the Monitoring Act, similarly to the inclusion of the phrase "or other interests", could open the door to abuse. MTN therefore submits that the wording "to the security of the Republic, and" be deleted in its entirety. Alternatively, that a clear, unambiguous definition of "security of the Republic" be inserted in Section 1 of the Monitoring Act. MTN notes that the Commission proposes that the judge concerned need only be satisfied that the grounds mentioned in a written application comply with the directives referred to in Section 6 of the Monitoring Act. MTN states that as previously mentioned, it is of the view that the watering down of the "onus of proof" so to speak placed upon the State, is inappropriate in the circumstances. Should a judge only need to be "satisfied" as proposed, MTN is of the view that the parameters of the judge's "satisfaction" be clearly established in the Monitoring Act. Vodacom remarks that the relative ease and technological capacity to obtain information in the way set out in the Act, necessitates that the standard set out in the current Act, should not be changed from the judge having to be *convinced* to being *satisfied*.

12.2.7.3 MTN notes also that the Commission further proposes that the phrase "another less intrusive" be inserted in clause 3(1)(b)(i). MTN notes that in this regard, in the United States of America law enforcement agencies must also demonstrate that other investigative techniques have failed or are too dangerous. The United States of America Congress made it clear in the 1968 Wire Tap Act that wire tapping was to be an investigative means of "last

resort". MTN favours this approach. MTN further notes that the Commission proposes that the phrase "all the interests" be inserted in clause 3(b)(ii). They also refer to their comments they made on clause 1(c)[44].

12.2.7.4 The Law Society's standing committee on constitutional affairs remarks that clause 3(1)(b) proposes that a judge needs only be "satisfied", as opposed to being "convinced", as stated in the Act, that the grounds listed in clause 3(1)(b) are present, before issuing a directive. The Law Society refers to the case of *S v Makoula* 1978 (4) SA 763 (SWA) at 768 E - F where it was explained that "convinced" sets a higher standard of proof than merely requiring a person to be "satisfied" of the existence of a fact or set of affairs. The Law Society's Committee submits that in light of the seriousness of the infringement of the right to privacy that may follow after directive is issued, the stricter standard of proof needs to be retained. The NICOC subcommittee however supports the substitution of the word "convinced" with the word "satisfied".

12.2.7.5 Judge Gordon[45] states that he agrees with the substitution of the term "convinced" which in his view is unsuitable. He notes that in the USA the phrase used is "probable cause" and in Great Britain "that the warrant is necessary". He states that he agrees with the term "satisfied". He remarks that this is a matter frequently discussed after he personally stated that the word "convinced" is unsuitable.

12.2.7.6 The National Intelligence Agency[46] states that they have also noted the inclusion of "state interests" as a possible ground for bringing an application. Cases do emerge from time to time where monitoring would be in the best interests of the State, but where it would not be possible to base applications on state security. The NIA considers that in view of the fact

---

44 The amendment proposed in the discussion paper is that the words "or other interest" be inserted in the definition. MTN is of the view that these particular words should not be inserted but should be deleted in their entirety. MTN remarks that such "other interests" without being very clearly defined, could include the political interests of the government of the day. MTN is of the view that the addition of paragraphs (c), (d) and (e) would in any event cater for all criminal activities that are perpetrated. MTN is of the view that, alternatively, the "other interests" should be very narrowly defined in the Act. MTN suggests that this would hopefully preclude any kind of governmental or political abuse that may be occasioned by the addition of the words "other interests".

45 Of the Office for Control of Interception and Monitoring of Communications.

46 Deputy Director-General Operational Services.

that a judge will be entertaining these applications, and will probably limit them to cases of important interests, they do not believe that this will open the door for abuse.

12.2.7.7 Adv Mnyatheli of the Investigative Directorate Serious Economic Offences states that in his view no harm is conceivable if the word interests of the Republic is used. He states that if the interests are economic interests it is not bad to say so and the courts are used to the use of the term interests of the Republic. He thinks the addition is necessary and any checks and balances may be gained by a judicial consideration, which will attend to each case on the basis of the merits it may present.

12.2.7.8 The DPP Investigating Directorate Organised Crime and Public Safety and the DPP Cape of Good Hope comments as follows in this regard:

> ... daar word aanbeveel dat daar uitdruklik in die wet bepaal word dat "satisfied" (tevrede) beteken op 'n oorwig van waarskynlikhede.

12.2.7.9 Ms Naicker[47] considers that the Commission's view is supported in that more attention should be given to the word "interests". She considers that the applicant must be clear on which interests of the Republic will be affected.[48] She notes that the possible categories are military/defence; economical/financial (fraud); political (international relations); social welfare (health) etc. She is of the view that the threshold that the judge must be convinced that an offence has been or will be committed is quite high. She therefore suggests that the standard should be that the judge is "reasonably satisfied" and not "convinced". Ms Naicker suggests that if the words "reasonably satisfied" are used it allows for a "qualified discretion" that the judge may have. She notes that the latter half of the paragraph which states that "the offence cannot be properly investigated in any other manner", should be amended. She notes that the American approach is a favourable one, which words a similar clause; as follows "normal investigative methods have been tried and have failed or reasonably appear to be unlikely to succeed or are too dangerous. She points out that the American clause places an onus on the State to show in what way the normal investigative procedures have failed or

---

47 Department of Public Works.

48 The NICOC subcommittee supports the inclusion of "interests of the State" in section 3(1)(b)(ii). They consider that the fact that a judge will have to be satisfied before granting a directive, should address fears of abuse. They suggest that it could be considered to qualify "interest" by means of the word "substantial".

are unlikely to succeed in comparison to the present method. It requires that the State show why this method would be the most suitable method and what results it is likely to produce that the usual methods could not produce. She also considers that further consideration should be given to the time some investigations take especially where the security of the State is at risk and urgent action needs to be taken.

12.2.7.10 The SAPS[49] remarks that the proposed amendment to section 3(1)(b)(i), namely the substitution of the words "any other" with "another, less intrusive" is strongly supported, but that it might, however, lead to legal uncertainty. In view of the elaborate definition of "serious crime"' the SAPS proposes that section 3(1)(b)(i) be amended as follows:[50]

> (i) that the offence that has been or is being or will probably be committed, is a serious offence **[that cannot be properly investigated in any other manner and]**of which the investigation in terms of this Act is necessary.

(b) Evaluation

12.2.7.11 The project considered the standard set by the proposed clause 3(1)(b)(i). It considered the wording proposed by the intelligence community and whether their suggested wording should be adopted, namely "that the offence that has been or is being or will probably be committed, is a serious offence of which the investigation in terms of this Act is appropriate". The committee noted that the discretion of what is appropriate, might very well embrace the range of alternatives that are available. The committee considered that it might therefore not be improper for the judge who is confronted with such an application to say: is this the most appropriate method? The committee considered the elimination, firstly of the less intrusive method and, secondly, the standard of assessment. The committee noted that there might very well be objections to a watering down of the required standard of assessment and that it might be argued that the right to privacy should be heeded. The committee took, however, into account, that it is not dealing in this instance with a 19th century method of search and seizure but with a modern one.

12.2.7.12 The project committee also considered the adoption of the standard set by the

---

49 Chief Manager: Legal Component Detective Services.

50 A proposal which is also made by the NICOC subcommittee.

wording of the Canadian statute, and whether the proposed clause should be elaborated by requiring that there should be reasonable and probable grounds for granting the application. The committee was of the view that the Canadian example is an appropriate safeguard. The committee noted that the approach of the Canadians and Americans in regard to search and seizure is compliance with essentially two requirements: firstly that a warrant be issued by an independent third party like a judge or a magistrate, and secondly, that the evidence on which the warrant is issued, must usually be given on oath. The committee took into account that this is one step short of evidence on oath because it requires the judge to be satisfied that there are reasonable and probable grounds to believe that an offence has been or is been committed and that the authorisation sought will afford evidence of that offence. The committee suggested that unless such safeguards of this sort are built into the Bill, in circumstances where one does not have the requirement of evidence on oath, it will in all probability be open to constitutional attack, whether it is justified or not. The committee was of the view that the section would be more constitutionality defensible with the inclusion of the Canadian wording. The committee noted that a judge might argue that in as much as he or she is required to be satisfied on the basis of reasonable and probable grounds, how is he or she going to do that and that the best way is to require an affidavit. The committee was of the view that the statute would be far more defensible on that basis as one would read it in such a way as to build in the constitutional safeguard.

12.2.7.13 The committee therefore resolved that section 3(1)(b) be amended to read as follows: "that there are reasonable and probable grounds to believe that a serious offence has been or is being committed and that the offence cannot be investigated in another appropriate manner" and that the words "any other manner and of which the investigation in terms of this Act is necessary" be deleted. The committee further resolved that subparagraph (ii) should amended by the substitution of the phrase "that the security or the interests of the Republic is threatened" by "that the security or the interests of the Republic are threatened".

12.2.7.14 The committee further considered whether the word "substantial" should be added to the term "interests" in section 3(1)(b)(ii). The committee considered that substantial interests would be difficult to define and did therefore not support the proposal.

12.2.7.15 The project committee also considered the suggestion that a clause be inserted into the Bill setting out that a judge may upon application direct further additions or amendments to

existing directives. The committee noted that the aim of the suggested provision is that where one wishes a directive to be altered that it is not necessary to bring a fresh application. The committee was of the view that this is a sensible addition, that it would permit an application to a judge who was originally seized with the matter and that it makes sense that the Act should make provision for the variation or amendment of existing directives.

12.2.7.16 The Commission agrees with the project committee's reasoning why section 3(1)(b) should be amended. The Commission however considers that the requirement should be that the judge is satisfied on the facts alleged in a written application that there are reasonable grounds to believe that a serious offence has been or is being committed and that the offence cannot be investigated in another appropriate manner. The Commission does not favour the inclusion of the additional requirement of "probable" grounds, as the project committee proposed. The Commission further agrees with the deletion of the words "any other manner and of which the investigation in terms of this Act is necessary" and the substitution in subparagraph (ii) of the phrase "that the security or interests of the Republic is threatened" by "that the security or compelling national interests of the Republic are threatened" (see par 12.2.3.35 above where the Commission argues that the wording "other interests of the Republic" is too vague and that provision should therefore be made in addition to offences which may harm the economy of the Republic for offences which may harm the "compelling national interests of the Republic"). The Commission also notes that where there is a need for an existing directive to be altered then it should not be necessary to bring a fresh application requesting the issue of a directive. The Commission is of the view that this is a sensible addition and that the Act should permit an application to a judge who was originally seized with the matter to amend an existing directive.

(c) Recommendation

12.2.7.17 The Commission recommends that section 3(1)(b) be amended to provide that the judge may issue a directive if he or she is satisfied that there are reasonable grounds to believe that a serious offence has been or is being committed or will be committed and that the offence cannot be investigated in another appropriate manner". The Commission further recommends that section 3(b)(ii) should be amended to provide "that the security or compelling national interests of the Republic are threatened or that the gathering of information concerning a threat to the security or compelling national interests of the Republic is necessary". The Commission

recommends further that a clause 3(8) be inserted into the Bill setting out that the judge may upon application direct further additions or amendments to an existing directive if he or she is satisfied that the addition or amendment is necessary.

12.2.8 Clause 3(7): client/legal representative privilege

(a) Comments on the proposed clause

12.2.8.1 The DPP Investigating Directorate Organised Crime and Public Safety and the DPP Cape of Good Hope comments as follows in this regard:

> Hierdie wysiging soos hy tans in die wysigingswet staan word nie ondersteun nie. Dit is respondent se respekvolle mening dat wat hier beoog word is om gepriviligeerde inligting uit te sluit. Dit is respondent se respekvolle mening dat die gemeenregtelike klient/prokureur priviligie genoemsame beskerming aan die klient bied. Wat egter problematies is met hierdie wysiging is dat indien die artikel soos hy tans staan in die finale wetgewing opgeneem word dit sal meebring dat waar daar magtiging bekom word om 'n spesifieke verdagte/beskuldigde se telefoon af te luister en sy regsverteenwoordiger hom toevallig skakel in verband met 'n ander aangeleentheid die opname van sodanige telefoongesprek eerstens 'n misdryf daarstel en tweedens die hele meeluistering en aanbied van getuienis kan kontamineer. Respondent is van mening dat kliënte en regspraktisyns genoeg beskerming geniet onder die gemenereg en dat regsadviseurs nie spesiale beskerming moet kry in gevolge hierdie wet waar hulle met kriminele aktiwiteite besig is nie. Om hierdie aspek tot sy ekstreme te illustreer kan daar na die volgende voorbeeld gekyk word. Sou daar inligting wees dat 'n betrokke regter hom besig hou met kriminele aktiwiteite. Sou dit geregverdig wees om die betrokke of die katagorie, regter spesiale beskerming in gevolge hierdie wetgewing te bied? Dit is respondent se respekvolle mening dat dit nooit regverdigbaar kan wees nie en derhalwe ook nie vir die kategorie van regsverteenwoordigers nie.
>
> Indien dit blyk dat enige regsverteenwoordiger, hetsy 'n prokureur of advokaat hom besig hou met kriminele aktiwiteite moet hy oor dieselfde kam geskeer word as enige ander verdagte. Respondent is van mening dat in alle gevalle waar daar 'n aansoek gebring word in gevolge hierdie wet daar gesteun moet word op "reliable information" en die invoeging van hierdie woorde in die artikel kan die indruk laat dat omdat 'n persoon 'n sekere rang of titel beklee in die gemeenskap hy voorkeur behandeling moet ontvang. Respondent is van mening dat sodanige uitsondering nie regverdigbaar is nie. Indien die regsverteenwoordiger en/of sy kliënt wil steun op die grond dat die inligting wat op band opgeneem is gepriviligeerd is, is dit in elk geval hulle goeie reg om dit te doen, ongeag of daar sodanige bepaling in die onderhawige wet is al dan nie.

12.2.8.2 The Law Society of SA's standing committee on constitutional affairs notes that in light of the breach of privilege this may entail, the communications between a legal representative and his or her legal representative should not be intercepted or monitored. The

Law Society's Committee considers that if this interception or monitoring is not prohibited, then a stricter standard of proof should be set. This could be done by either requiring the judge to be convinced" (rather than merely "satisfied") that such a legal representative is "involved in, or aiding or abetting a serious offence" or requiring the judge to be satisfied that the legal representative actually committed a serious offence.

12.2.8.3 Judge Gordon[51] states that he agrees to adding the additional subparagraph (7) but adds that there is no difficulty in dealing with an intercept or monitoring with a legal representative where the application discloses the suspicion of a communication between such parties. He remarks that where there is no reference to the fact that one of the parties to the communication (conversation) may be a legal representative, or no suspicion of such fact, a direction, if otherwise in order, would be granted and monitoring would take place. Since direct listening-in does not take place, it may only thereafter be ascertained that a legal representative was one of the parties to the conversation i.e. after the monitoring has been done since it was not known in advance that this would be the case. Judge Gordon points out that in such a case, in the United States of America the monitoring agent has to "minimize"; i.e. disclosure or use of the recording is limited to those communications that are criminal in nature. This is precisely what happened in the *Nkabinde* case. Hence the order made by him contains the "non disclosure" injunction which was "after the fact minimization" (to use the USA expression). Judge Gordon considers that these are matters which may also conveniently be dealt with in the Rules and no further addition to the section being necessary.

12.2.8.4 The SAPS[52] states that they honour the client-legal representative privilege but consider that an absolute prohibition on the monitoring of this communication posses several practical problems. The SAPS states that in practice this total prohibition would mean the means of monitoring and interception should be switched off for the duration of the conversation and that should this happen it will not be known when the conversation ends and monitoring can therefore be re-assured. The SAPS remarks that in practice monitoring is also a continuous process with the recording taking place without a person always physically listening. The SAPS points out that although they are aware of the order which was issued following the unreported Natal decision (*S v Nakabinde*) they are of opinion that there should not be a total

---

51 Of the Office for Control of Interception and Monitoring of Communications.

52 Chief Manager: Legal Component Detective Services.

prohibition on the monitoring on conversations between a client and the legal representative but that evidence obtained in such a way should not be acted upon or relayed to the investigation officer and should at all times be inadmissible as evidence in a court of law.

12.2.8.5 The SAPS notes that it is practically impossible to do "live" monitoring of each and every conversation which may be monitored. "*Monitor*" in terms of the Act, also includes the *"recording"* of a communication. The SAPS states as mentioned above, in most instances the communications on a telecommunications line (number) is being monitored by recording. The SAPS points out that at an opportune time the recordings are listened and sifted for relevance and only relevant communications transcribed. The SAPS considers that another aspect which is worrying and which could be addressed, is the fact that in the process it might happen that another person uses the telephone i.e. a person in respect of which there is no authorization to monitor the conversation or communication. It might be a person completely detached from the crime which is being committed, or it might be an accomplice, furthering the illegitimate purposes of a syndicate leader. The SAPS notes that naturally the information gleaned in the process in respect of an uninvolved person is protected by the provisions of section 7 of the Act, and will not be divulged for any reason. The SAPS considers that it can also be argued that no offence has been intentionally committed by the recording. The SAPS considers that a solution could be to only stipulate in the Act that information of a privileged nature obtained through interception and monitoring may not be used as evidence in a trial.

12.2.8.6 Vodacom considers that the same standard as set out in section 3(1)(b) should apply in respect of communications between legal representatives and their clients, ie that the Judge should be *convinced* that the legal representative is involved in, or aiding or abetting a serious offence.

(b) Evaluation

12.2.8.7 The project committee considered the proposed clause and was of the view that there is a need to retain it. The committee however resolved that the clause should be brought into line with the standard of assessment it proposed should apply in respect of clause 3(1). The committee therefore decided that the phrase "except if on reliable information, the judge is satisfied" should be substituted with "except if on reasonable and probable grounds the judge is satisfied".

12.2.8.8 The Commission agrees with the project committee that there is a need to regulate attorney/client privilege in the Act and that the same standard of assessment should apply in this clause as in section 3(1). The Commission however considers that the standard should be one of "reasonable grounds" and not "probable" grounds as well. The Commission further considers that the clause should be amended to apply in respect to security matters too and not only serious offences.

(c) Recommendation

12.2.8.9 The Commission recommends that the Act should regulate attorney/client privilege and that the clause should provide that no communication between a legal representative and his or her client may be intercepted or monitored, except if on reasonable grounds, the judge is satisfied that such a legal representative is involved in, or aiding or abetting a serious offence or an offence threatening the security of the Republic."

12.2.9 Clause 4(5): the remuneration shall only be in respect of direct costs

(a) Comments on the proposed clause

12.2.9.1 Telkom notes that "direct costs" are not defined and should preferably be more fully described. Telkom remarks that the following basic costs are currently charged by Telkom for services rendered:

Once off:
(i) Basic connection - R 80,77
(ii) Connection per exchanges R 622,44 (if applicable).
Monthly:
- Direct distance between connection and monitoring - R 7,64 kilometer
- Basic facility to monitoring center - R 47,65 / month Information regarding users:
  - Name/address/ID - R 3.17
  - Detail billing - R 3.1 7/ page

12.2.9.2 Telkom states that the following costs are as yet not charged for by Telkom:

- Staff salaries, overtime (if needed), transport, travelling cost, security clearances, security on of f ices, fax machines, cryptography equipment, safes, computers, offices space, telephone calls, witness fees etc.

12.2.9.3 Telkom considers such costs are directly linked to the provision of the service and

should be included in the remuneration, payable to the telecommunications service/network provider. Telkom states it should as a minimum be allowed to amortise the cost of any equipment purchased for the purposes of this Act, over the technical life of the equipment and include such cost into the cost of the leased circuits or the cost of providing the specific service.

12.2.9.4 MTN notes that the suggested amendment indicates that only direct costs incurred in respect of personnel and administration and the lease of telecommunications lines, where applicable, may be received from the State by the Network Operator concerned. It furthermore states that it shall not include the costs of acquiring the facilities and devices referred to in Section 5A(2). MTN states it is dismayed at the fact that the costs of these facilities and devices that need to be acquired to do the necessary interception or monitoring as required by the proposed Bill, may not be redeemed from the State. The cost of such facilities and devices for a company such as MTN would be in the region of Multi-Million Rands. MTN points out that it is stated in Chapter 11 of the Law Commission report that it may easily be that if the State assumes responsibility for these costs, that the State will keep on paying tremendous amounts only to keep track with technology, which is renewed every few months and that this argument is equally applicable to a company such as MTN.

12.2.9.5 MTN states that the further proposed amendments contained in Section 5A(1) suggest that a communications company may not provide any service which is not capable and does not have the capacity to be monitored. MTN is of the view that placing such an obligation on MTN is an effective amendment of its Licence and such amendment is proposed outside of the normal processes and procedures as contained in the MTN Licence as well as the Telecommunications Act.

12.2.9.6 MTN suggests that the concept of direct costs as contained in the suggested sub-section (4) needs to be assessed. Currently, MTN is of the view that such direct costs would relate to providing the security to the room from which such interception and monitoring is being done, costs related to the security clearance of personnel dealing with Act 127 directives, salaries of personnel of the Network Provider dealing with such directives, over-time payments to such personnel, office space, cryptography equipment, transportation of documentation and personnel, telephone calls made by Network Operators personnel as well as the time spent by personnel in any court cases. MTN notes that clarity needs to be provided as to whether this is indeed the intention of the proposed Bill.

12.2.9.7 MTN considers that it should further be noted that by placing such an obligation on the Network Operators to obtain the necessary facilities and equipment, such costs will necessarily be devolved upon the consumer. MTN points out that Network Operators are however, in terms of their Licence conditions, obliged not to increase their tariffs by more than a certain percentage year on year. MTN remarks that the Network Operator, would therefore be placed in a position where government places an extra burden on such operator and yet, through a Licence by the same Government, not allow such Network Operator to efficiently operate its business. MTN considers that in this sense government would be able to interfere with the commercial freedom of a Network Operator. MTN submits that the telecommunications industry must be satisfied that the cost of providing intercepts should not become an undue burden on companies and that the number of intercepts will be of such a nature that:

- it would require law enforcement to focus on what it actually requires to accomplish it's legitimate needs thereby freeing resources that they do not actually require for other purposes;
- To provide an essential mechanism for the government to control both the costs and level of law enforcement involvement in the development of new services;
- And to ensure that the fewest tax payer Rands are spent to address law enforcement concerns.

12.2.9.8 MTN states that it is of the view that, *inter alia*, the following goals should be realised:

- Costs to consumers are kept low, so that "gold-plating" by the industries is kept in check;
- The legitimate needs of law enforcement are met, but that law enforcement does not engage in gold plating of its demands;
- Privacy interests of all South Africans are protected;
- The goal of encouraged competition in all forms of telecommunications is not undermined, and the fact of compliance is not used as either a sword or a shield in realisation of that goal.

12.2.9.9 MTN notes that in the USA, similar legislation ("CALEA"), faced strong opposition from industry and civil liberties organisations in the US and that the legislation was however adopted in the closing hours of Congress after the Government offered to pay telephone companies $ 500 million to make the proposed changes. MTN states that it should also be noted that the Congress approved a provision allowing for funding the CALEA from money reprogrammed from intelligence and law enforcement agencies. MTN points out that due to the controversies surrounding the CALEA, the Federal Communications Commission granted

an extension of the compliance date of the systems capability requirements to June 30, 2000.[53] MTN is of the view that the annual Licence fees payable by MTN to the Government would be adequate to cover the implementation of the requirements of the current Monitoring Act. MTN also notes that in the UK, Lord Nolan, Interception of Communications Commissioner reported that 1 712 phone and mail interceptions were issued in 1997, compared with 1 307 in 1996. A total of 1 647 phone taps were issued during 1997 at 25% rise on the 1996 figure of 1 301. MTN notes that the surveillance included the tapping of several law biding members of the public whose phones were bugged by mistake after operators got the wrong numbers.

12.2.9.10 The SAPS[54] comments that the intention should be that the service providers should be responsible for the costs of equipment, software, etc., whilst the costs for the services rendered should be borne by the government departments (personnel and administrative costs). The NICOC subcommittee considers that the service providers should be responsible for the costs of software and/or hardware, whatever applicable/possible on their own equipment to effect monitoring, and all necessary interfaces to their equipment to route duplicated communications to the recording equipment (monitoring centres). The NICOC subcommittee suggests that the SAPS, NIA, SASS and SANDF should be responsible for costs of monitoring and recording equipment in the monitoring centrres, leasing of lines from premises of service providers to monitoring centres, and the services delivered by the service providers at a tariff to be determined on the basis of agreement or, if no agreement is reached, determined by the Minister of Posts and Telecommunications.

12.2.9.11 Vodacom notes that it does not view the provision of these facilities, devices and services as an opportunity for commercial gain but as a service to the country, and will be rendered on a cost-orientated basis. Thus, Vodacom points out that it does not support the Commission's recommendation that the costs related to the procurement of the monitoring and interception equipment, as well as the provision of the facilities and services, for the account of the telecommunications network operator. Vodacom notes that the Act currently makes provision for "reasonable remuneration" to be paid to the network operator. Vodacom submits that "reasonable remuneration" in all cases would include a capital component plus interest, maintenance and other variable costs and that there is no reason to change this approach.

---

53 Which was extended again to October 2000.

54 Chief Manager: Legal Component Detective Services.

Vodacom is of the opinion that the Act allows for the following fair remuneration to be paid to network operators:

- A fixed monthly charge by which the network operator will be compensated over time for the cost of procuring and upgrading the facilities and equipment (including software) and the initial installation and connection to the same network (this will include interest on capital).
- Monthly variable costs related to the operation and maintanance of the system, rental of office space, salaries, security clearance, training for personnel and so on.

12.2.9.12 Vodacom suggests that the costs related to the State's duty to protect the security of the Republic and to investigate crime must be paid from the fiscus and not carried or transferred onto the telecommunication operators, and ultimately their customers. Vodacom submits that the tax revenue and licence fees paid by telecommunications network operators into the National Revenue Fund will adequately cover the cost of the implementation of the Act. As for the availability and potential costs of various facilities and services, Vodacom suggests that the Commission hold separate discussions with Telkom, the existing mobile cellular operators, Internet service providers and VANs, and so on. Vodacom requets that representatives of the Department of Communications and SATRA be present. Vodacom points out that the total cost to the State will depend on the demand for the facilities and that Parliamentary oversight is thus also important to ensure that the various agencies do not over-utilise these facilities and services.

12.2.9.13 Ms Naicker[55] states that her Department is not in a position to levy any comment on the issue of the direct costs that are involved and the monetary implication thereof. She however considers that the onus, which is placed on the Network Providers to provide the investment, technical maintenance and operating costs, in order to make that telecommunication service capable of being monitored is burdensome. She considers that at the outset the installation of such equipment would be expensive, as well as the future maintenance thereof. She states that it is important to place a duty on the Network Providers to maintain the equipment because the State does not have the financial resources to do so.

---

55 Of the Department of Public Works.

She suggests that at the outset a policy document should be formulated in order to help subsidise the initial installation of such equipment. Ms Naicker points out that the main users of the information by way of monitoring will be the State and after the equipment is set-up the duty of maintenance shall rest with the Network Provider. She suggests that this assistance from the State in the initial phases will add legitimacy to the possible fines or revocation of licences in instances where the network is not maintained by the Network Provider. She considers that the Minister's directive in terms of section 5A(6) would therefore be more acceptable as the initial set-up will not have been too burdensome on the Network Providers. She considers that if unduly harsh restrictions are placed on Network Providers without the assistance of the State this may affect the possible development in this field.

12.2.9.14 M-Web states they object to the proposed imposition of an obligation on telecommunications services licensees to bear the expense of procuring the necessary facilities and devices for monitoring and interception. M-Web states that this proposed obligation purports to impose a *'tax'* on the licensee to subsidize an expense which is properly borne by the State. M-Web remarks that careful regard should be had to the fact that telecommunications licensees are not only burdened by income tax legislation in the ordinary course but may also be required by the Telecommunications Act No. 103 of 1996 to pay licence fees, human resource fund levies, and universal service fund levies. in particular, in the provision of value added network services (including Internet services) the market is extremely competitive and any further financial burdens on investors in this burgeoning industry may undermine the development of the sector. M-Web notes that Government has already recognised the role that telecommunications service licensees can play in the overall economic development of South Africa and its citizens and this should not be undermined by the policy considerations driving the proposed changes to the Act.

12.2.9.15 Judge Gordon states that when it is proposed to legislate on costs to be incurred by commercial firms and service providers, especially when these costs are unknown and are to be incurred for State purposes (to investigate crime) every effort should be made to come to terms with these business firms. He remarks that if no agreement is reached it seems clear to him that adequate notice must be given to *every* interested party of the proposed legislation and to give the parties an opportunity formally to lodge objection.

(b) Evaluation

12.2.9.16 The project committee noted that there are presently negotiations being conducted involving, inter alia, the Intelligence Agency and the cellular telecommunication operators. The committee noted that a legitimate debate is conducted as to where the costs should lie in regard to the financial implications which will result from the proposed amendments, should they be effected. The committee took into account that on the hand, the present cellular operators and Telkom take the attitude that they pay their taxes and that the revenue derived from these taxes should be appropriately directed. The project committee was advised by these parties that law enforcement, of which the Interception and Monitoring Prohibition Act is a part, is quintessentially a function of the State. The committee also noted the opposing view that telecommunications operators are in possession of a very productive and lucrative resource, and that it is therefore appropriate in those circumstances that they should bear particular obligations. Having further regard to modern technology and criminal methods, including the use of their products, the committee considered that it is entirely appropriate that the telecommunication operators should bear the costs. The committee also suggests that this is an indeterminable debate which will not be resolved by the Commission.

12.2.9.17 The project committee was therefore of the view that the Bill should provide that the costs in regard to acquiring the facilities and devices referred to section 5A(2), should be borne by the cellular operators. The committee therefore proposed, as was proposed in the discussion paper, that the remuneration referred to in sections 5(2) and (3) payable to a person, body or organisation who made a facility, device or telecommunications system available under the Act, shall only be in respect of direct costs incurred in respect of personnel and administration and the lease of a telecommunications system, where applicable, and shall not include the costs of acquiring the facilities and devices referred to section 5A(2).

12.2.9.18 The Commission concurs with the project committee and its reasoning why telecommunications operators should bear the costs of acquiring the facilities and devices concerned. The Commission also agrees with the wording of the recommended clause.

(c) Recommendation

12.2.9.19 The Commission recommends that telecommunications operators should bear the

costs of acquiring the facilities and devices concerned and that remuneration payable under the Act should be in respect of direct costs incurred in respect of personnel and administration and the lease of telecommunications system, where applicable.

12.2.10 Clause 5A: ensuring capacity to intercept

(a) Comments on the proposed clause

12.2.10.1 MTN notes that the proposed clause 5A(1) obliges an organisation rendering a telecommunication service only to provide those services which are capable of and have the capacity to be monitored. MTN considers that this would place an unreasonable obligation on any Network Provider to be able to decipher any kind of encryption on its Network. MTN points out that as an example Person A using the network of a Network Provider phones Person B while both parties to this conversation attach encryption devices to their telephone instruments. The communication or conversation would therefore be sent over the telecommunications line in an encrypted format. MTN notes that the Network Operator who has provided the Network over which such communication takes place, would therefore be obliged in terms of the current wording to decrypt any such encryption, no matter what it was. MTN remarks that each and every manufacturer of the encryption devices that may be able to be used over telecommunications networks would therefore have to be approached by the Network Operators to obtain the decryption codes of those encryption devices and that clearly this cannot be the intention of the legislature.

12.2.10.2 Reuters remarks that the discussion paper does not say whether it is proposed to prohibit or limit the use of encryption by those who use telecommunications services. Reuters request clarity whether it is proposed to make it an offence for the customers of telecommunications services to use encryption techniques. Reuters notes that businesses are generally opposed to restrictions on encryption technology, whether these relate to import, export or usage controls, or government key recovery schemes. Reuters points out that companies want to use encryption, including strong encryption, to protect the privacy and integrity of their data and to restrict encryption would undermine attempts to build trust in electronic commerce and other on-line services. Reuters states that without this trust, the potential of this emerging sector of the economy will not be realised. Reuters notes that the case is made that use of encryption by criminals may make it more difficult to obtain intelligence

by means of encryption. Reuters notes that the real question to be answered is will legal restrictions on encryption make interception more effective? Reuters state that they have not heard a compelling argument that it will. Reuters considers that it can instead be argued that serious criminals will use strong encryption techniques regardless of legal restrictions and that the practical effect of legislation that restricts encryption would be to penalise law-abiding businesses and citizens, whilst only improving intelligence gathering against relatively minor criminals.

12.2.10.3 The Joint Communication Security Council and the SA Communication Security Agency state that while the section entitled "Background" of Chapter 1 of Discussion Document 78 mentions cryptography, the amendment Bill does not address this problem at all. They note that the use of cryptographic methods to ensure the privacy, authenticity and integrity of communications is common, and in fact forms an essential part of electronic commerce, both consumer-to-business and business-to-business. They state that cryptography is readily available:

- Strong encryption algorisms for private or business use, such as PGP, can be obtained, free of charge, from the Internet. (PGP is a 64 bit block cipher, using a 128 bit key, and must be considered unbreakable.)
- Virtually Private Networks (VPNs) are coming into common usage: all communication over such networks is encrypted.
- At the insistence of the users, protocols and algorisms to ensure privacy are becoming the norm in electronic commerce (and to a limited extent in personal communication): a number of different standards have already established themselves, such as SET, S/MIME, SSL, SHTTP, Ipsec, with Ipv.6 as a standard in a preparation.

12.2.10.4 The Joint Communication Security Council and the SA Communication Security Agency note that the fact that the same techniques can be used by terrorists and other criminals is an unfortunate corollary. They remark that as the Amendment Bill stands, the obligation of the service provider ends with providing interception and monitoring facilities; there does not appear to be an obligation to provide the law enforcement and national security agencies with the plaintext of any communication. They consider that consequently, law enforcement and national security agencies will in many cases only have access to encrypted data, and it is important that they be aware of the fact that they find themselves in a totally different position from that that prevailed in the past when telephone wiretapping was feasible: the decryption of encrypted data cannot be done in real time. (Recently a *custom built* $250

000 DES-cracker found a 56 bit Des key in approximately 22 hours, the current record.)

12.2.10.5 The Joint Communication Security Council and the SA Communication Security Agency state that some provision for lawful access (ie under a suitable court order as in the Interception and Monitoring Prohibition Act of 1992) needs to be made: the concept of compulsory key escrow, or preferably compulsory key back-up, needs to be considered.

12.2.10.6 The Joint Communication Security Council and the SA Communication Security Agency consider that it needs to be clearly understood that any system that allows for lawful monitoring of communications introduces new vulnerabilities: the same system that allows access to law enforcement agencies can also be misused by adversaries to gain access to the same communications. They state that the fact that any information gathered in this way may only be provided to certain agencies (SAPS, SANDF, etc) is no guarantee that it will not be provided to others. They note that in the case of the Department of Defence, which uses a commercial carrier for much of its communications, the dangers are obvious: the service provider will become an obvious target (for example through subversion of the service provider's personnel) for hostile forces. They remark that even if the communications are encrypted, traffic analysis remains a possibility: the information required from service providers as "call-related information" under section 1 of the (amended) Act provides an ideal basis for such analysis. They remark that in the case of commercial traffic, the possibility of economic espionage by competing businesses cannot be discounted: it is widely rumoured that even some foreign governments are actively involved in such activities. Again, the back-door provided by compulsory provision of access will be a tempting target. They point out that the vulnerability of the DoD's communications through the introduction of compulsory "back-doors" has already been mentioned. They state that the point has been raised that the SA Army, in the course of its monitoring of military wireless traffic, may accidentally pick up local non-military traffic and thereby contravene the Act. The Joint Communication Security Council and the SA Communication Security Agency note that as long as this happens accidentally, ie as long as there is no deliberate invasion of privacy, and the content of such traffic is kept confidential (and destroyed as soon as possible) this should not create a problem. They suggests that the Act should nevertheless perhaps specify how such an eventuality is to be handled.

12.2.10.7 Mr Paul Sheer[56] remarks that it is trivial for two parties to communicate using encrypted channels over the Internet. He notes that such encryption software is freely available (at no cost and having essentially no copyright, patent, or licensing restrictions) on the Internet, and exists in strengths that make it absolutely impossible to eaves-drop on. This software is essential to the operation of many companies who use the software to provide security from computer vandals (hackers), industrial espionage and fraud, which would otherwise be impossible to prevent against or even to detect. He recommends that this issue be given substantial attention, to the extent perhaps of even drafting an Internet Communications Act. He notes that the Internet represents such a radical departure from traditional communications that it warrants a thorough investigation in itself. He points out that legislation drafted in other countries often failed to consult with the relevant expertise in the areas of Internet communications and cryptography, and therefore fell short or instituted unfair and constricting limitations to industry. He states that the continued unrestricted use of secure, `un-eavesdrop-able' systems, in particular, will eliminate fraud, reduce banking transaction overheads, and stimulate trade. He notes that it can further provide substantial revenue where such systems can be developed within South Africa and sold abroad. He considers that the legislature should therefore be very careful not to place undue restrictions on communications; restrictions that may ultimately have the opposite effect with respect to crime control and prevention. He also recommends that the `free software community', that supports the responsible use of Internet communications and cryptography, should be consulted on these issues, since they are having a substantial impact in the computer industry (and indeed the entire economy), and have valuable expertise and opinions.

12.2.10.8 Vodacom notes that the Commission's recommendation and the draft Bill's provisions would prohibit the rendering of telecommunications services which are "not capable or do not have the capacity to be monitored". Vodacom submits that a statutory obligation to guarantee the interceptability of all products and services prior to the launching of such products or services, will have a tremendous negative impact on technological development in the telecommunications industry. Vodacom is of the opinion that the Act cannot and should not oblige a network operator to have the technical ability to decrypt (or decompress or otherwise manipulate) all conversations and communications moving across its network, when these

---

56 Of the company Obsidian Systems, see also his and his colleagues' comments on the definition of "call-related information" under par 12.2.1 above.

communications are being encrypted or otherwise made impervious to "unauthorised access" by users themselves. Vodacom considers that encryption techniques develop on a daily basis, and no telecommunication system operator can be expected to have all of the various types of decryption equipment available, if they exist at all. Vodacom states that the costs would be high, and would increase the cost of telecommunication services substantially. Vodacom remarks that for example, it is reported that the FBI spent $200m on a Cray Supercomputer to perform decryption and a single decryption can take up to a month to carry out. Vodacom states that it should also be noted that the cost of employing and training sufficient personnel to provide this type of service would be very high. Thus, Vodacom submits that the Bill should provide that the State agencies themselves should be responsible for the decryption of communications and conversations that are being monitored.

12.2.10.9 Telkom notes that two concepts are introduced by the Draft Bill, namely capability and capacity, that give rise to different sets of problems:

(a) capability to be monitored: the system must have such characteristics and functionality that monitoring of a specific conversation, communication or call-related data is possible, conversely it may not have characteristics or functionality specifically aimed at preventing monitoring, unless these can be overcome;

(b) The words "does not have the capacity (of service) to be monitored' - is not clear! Presumably it means that it should be possible to monitor any number (or a specified number) of conversations, communications and call data, without running into capacity problems. It is suggested that the intention should be made more clear.

12.2.10.10 Telkom suggests that the following issues pertain to capability:

(a) it is not clear what is meant by being "capable to be monitored':

(aa) Does it mean that it must be possible to uniquely access the signals pertaining to a specific conversation or communication, or the relevant call-related data, and reproduce them unaltered, and store them or transmit them to a predefined destination, or

(bb) that the signals so accessed must also be converted from the form in which they are at the point in which they are accessed, to a form that will permit an easy understanding of their information content by the person finally receiving them before they are stored or retransmitted (e.g. decryption of encrypted voice, representation of call data in a text form, etc.);

12.2.10.11 Telkom notes that if (bb) applies, the onus on the service provider is much higher than if (aa) applies, and in some instances it may be altogether impossible to meet, as for instance if the signal has been encrypted, or is in a proprietary transmission protocol, before it enters the network or facilities of the service provider. Telkom asks at which point in the network must the capability be provided: (aa) whether the signals can be monitored at a point where the communication line associated with the signal to be monitored is a single pre-identified facility (e.g. single-line local loop, single frequency radio link), or (bb) whether it is necessary to monitor the conversation at a point in the network hierarchy where the signal in question is mixed in an unpredictable manner with other similar signals (e.g. on the trunk side of a switching system):

12.2.10.12 Telkom remarks that in the first case accessing the signal is usually fairly straightforward, but in the latter case various degrees of complexity may be encountered, depending on the underlying technology used (e.g. analogue, digital time multiplexing, statistical multiplexing, etc.) the nature of the network (e.g. circuit switched, packet switched, fixed wire, mobile cellular, etc.). Telkom states that the following issues also pertain to capacity:

(a) to what extent and to what accuracy demand is predicted, and who is responsible for the forecast;
(b) the nature of the resources required, e.g. telecommunication lines to connect to the monitoring centres, computing resources in an exchange to access and/or process a signal, personnel, etc.

12.2.10.13 Telkom therefore considers that for all the above reasons, the absolute provision stipulated in this subsection needs to be moderated by some "reasonable endeavour" or similar provision, which should take into consideration embedded technology and the technical and financial capability of the service provider in relation to what may be required to meet this obligation. Telkom suggests the following amendment:

> 5A(1) Notwithstanding the provisions of any other law, no person, body or organisation rendering a telecommunication service may, <u>to the extent that it is both technically and economically feasible,</u> provide any such service which is not capable and does not have the capacity to be monitored.

12.2.10.14 SATRA notes that telecommunication services (within the broad meaning of the term) that are not capable of being be monitors with present technology, are already available. SATRA acknowledges that jurisdictions such as the United States of America do prohibit the

provision of telecommunication services that are not capable of being monitored and that such provisions have withstood Constitutional attack. SATRA considers that provisions that prohibit such telecommunication services are not entirely desirable in the global market where secure online of transaction are essential for electronic commerce. SATRA remarks that electronic commerce is not only about online shopping but it includes a large array of other activities. SATRA notes that business-to-business transactions on the Internet are big business and the costs of every day transactions are vastly reduced when conducted electronically on the Internet. SATRA states that a number of companies are focussing on electronic bill presentment and that electronic banking is reality.

12.2.10.15 SATRA remarks that prohibitions on the latest technology merely on the basis that it cannot be monitored would cause South Africa to lag behind it competitors. SATRA considers that less than world class technology could put South Africa, a so-called emerging market at a major technological and cost disadvantage - unable to trade due to technological inferiority and unable to compete because substantial cost savings available in the electronic market place are lost. SATRA suggests that South Africa's technological development would be severely handicapped by such provisions prohibiting telecommunication services that are not capable of being monitored. SATRA notes that the absurd result is that new technology cannot be introduced until such time, as a means of monitoring that technology is developed - it is analogous to prohibiting the introduction of the telephone until tapping devices are perfected. SATRA considers that, in this regard, the comments of Dr Duncan Chappell quoting the authors of *Crime in the Digital Age* (quoted on page 8 of the discussion document) are apposite:

> The advent of digital communications, combined with global trends towards privatisation and deregulation of the telecommunications industry, have posed new challenges for law enforcement. A proliferation of carriers and service providers make it difficult to discern which one to approach for assistance in undertaking surveillance of a particular target. Moreover, telecommunication systems can be designed to be more or less accessible to interception...
> As if the above challenges were not formidable enough, they in turn are compounded by the increasing accessibility of encryption technology..
> In addition to encryption, law enforcement agencies are concerned about the development and convergence of other technologies such as digital compression, highspeed data links, multiplex cable and synchronistic transfer mode technology. These all contribute to reducing law enforcement access to voice and data transmissions. The democratisation of telecommunications technology that is, its widespread accessibility to ordinary citizens, has begun to make many traditional law enforcement techniques obsolete.

12.2.10.16 SATRA notes that there is no turning back. SATRA asks whether South Africans should be denied the use of telecommunication services such as those provided by Iridium (a new telecommunications service provider that makes use of 66 low earth satellites) on the basis that those services cannot be monitored? SATRA asks whether it is not a natural consequence of development in telecommunications technology that communication become increasingly difficult to intercept? SATRA suggests that in addition, if strict standards of privacy are not adhered to, South Africa may find that it may not be able to conduct trade with the EU states. SATRA points out that as of October 1998 a new privacy policy known as the European Data Protection Directive is being implemented and any country that trades information with any of the EU states will be required to embrace Europe's strict standards of privacy protection. SATRA states that European countries will not be allowed to send personal information to countries that do not maintain adequate standard of privacy and thus countries such as the USA, that prohibits not only telecommunication facilities that are incapable of being intercepted but also robust encryption technology, could find themselves unable to access personal data relating to almost half of the developed world.

12.2.10.17 SATRA considers that if a statute were to prohibit unmonitorable telecommunication services, consumers of telecommunication services would then make more use of encryption technology thus ensuring privacy at the source by encrypting all outgoing messages before they are sent. SATRA considers that legislation that compels the users of encryption technology to provide monitors with a "key"to the encrypted telecommunication needs to be formulated so that encrypted messages can be intercepted and decoded. SATRA says that it realises that if telecommunication services that cannot be monitored are permitted these lines of communication may be used for criminal communications. SATRA considers that this can only be balanced against the concern that South Africa will be able to compete in a global computerised market with up to date technology at its disposal. However, developments in monitoring technology does tend to follow on the heels of developments of "secure"communications technology. SATRA remarks that if telecommunication service providers are required to invest in and develop monitoring facilities in terms of their licence conditions then allowing telecommunication services that cannot be monitored can, to some extent, be justified as telecommunication service providers will be required to invest in development of monitoring facilities for those communications that have yet to be capable of interception and monitoring.

12.2.10.18 The NICOC subcommittee considers that the obligation in the proposed subclause 5A(1) should be qualified by setting out that a service provider will not be obliged to decrypt any encrypted communication unless such encryption or the decryption forms part of the service concerned. They remark that this will apply to the providers of a so-called "secure line", and not to service providers providing an ordinary line carrying a communication which is encrypted at the one end, and decrypted at the other, by the users. They state that they assume that the ministerial powers provided for in subclauses (2), (6), (7) and (8) will be exercised only after consultation with interested parties.

(b) Evaluation

12.2.10.19 The project committee was of the view that it is not entirely clear whether there is a difference between the terms "capacity" and "capability" used in the proposed clause. The committee considered that a instrument is probably either capable or not to be monitored. The committee noted the comment by Telkom which suggests that this aspect be qualified to the extent that no person, body or organisation rendering a telecommunication service may, to the extent that it is both technically and economically feasible, provide any such service which is not capable and does not have the capacity to be monitored. The committee was not persuaded by their proposal. Subject to the project committee's reservation on the question whether there is a difference between capacity and capability, the committee was of the view that the clause should be retained.

12.2.10.20 The project committee considered that the wording of the clause should be amended by adding to the phrase "any such service which is not capable" the words "of being monitored". The committee decided that the wording "and does not have the capacity to be monitored" should be retained. The committee resolved that the draft report should reflect that it is not clear to it whether there is any need to distinguish between capability and capacity.

12.2.10.21 The Commission noted, inter alia, that the Australian terminology used in this context is "interception capability" and that while all carriers and carriage service providers are required to provide interception facilities, the Australian *Telecommunications Act 1997* also requires carriers and certain nominated carriage service providers to submit an annual Interception Capability Plan (ICP) setting out their policies in relation to interception generally

and their strategies for complying with their obligations.[57] The Commission further notes that the Australian Communications Authority's ICP deals with decrypting and decoding providing that where a carrier or carriage service provider modifies the call content,[58] the carrier is responsible for restoring it to its original form before transmitting it to the intercepting agency and where a target[59] modifies the call content of a call by encoding or encryption or by applying any other process, it is the responsibility of the intercepting agency to extract intelligence from the call. The Commission also considered the applicable American provision[60] which provides that a telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication. The use of the term "capability" was also noted.[61]

---

57 The carrier or carriage service provider is also required to give advance notice of proposed developments which could have an effect on their interception capability during the subsequent five years. The idea behind the ICPs is to provide a basis for carriers and agencies to think about and work through the implications of strategic business developments for interception capabilities and related matters. In the process of working through the implications, it is expected that agencies and carriers will identify for each service or category of service, an agreed interception capability which will enable the carrier to seek exemption from those elements that are not required. Interception Capability, in relation to a carriage service that involves, or will involve, the use of a controlled network or controlled facility, means the capability of the network or facility to enable a communication passing over it to be intercepted.

58 "Call content" is defined as any information transferred between a calling party and called party or parties in any form during a call.

59 "Target" or "intercept subject" is the person or persons identified in the warrant for interception and whose communications are to be intercepted.

60 Section 1002 of the US Code Title 47.

61 Sec. 1002. Assistance capability requirements:
(a) Capability requirements: Except as provided in subsections (b), (c), and (d) of this section and sections 1007(a) and 1008(b) and (d) of this title, a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of -
(1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government;
(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier -
(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
(B) in a manner that allows it to be associated with the communication to which it

The Commission further notes that the intelligence, security and policy agencies argue that a service provider will not be obliged to decrypt any encrypted communication unless such encryption or the decryption forms part of the service concerned. They remark that this will apply to the providers of a so-called "secure line", and not to service providers providing an ordinary line carrying a communication which is encrypted at the one end, and decrypted at the other, by the users. The Commission also notes that recent trends in international law and policy point toward continued relaxation of controls on cryptography,[62] but that a European

---

pertains,
except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18), such call-identifying
information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number);

(3) delivering intercepted communications and call-identifying information to the government, pursuant to a court order or other lawful authorization, in a format such that they may be transmitted by means of equipment, facilities, or services procured by the government to a location other than the premises of the carrier; and

(4) facilitating authorized communications interceptions and access to call-identifying information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects -

(A) the privacy and security of communications and call-identifying information not authorized to be intercepted; and

(B) information regarding the government's interception of communications and access to call-identifying information.

62 *Cryptography and Liberty 1999: An International Survey of Encryption Policy* Electronic Privacy Center Washington DC:

Most countries in the in the world today have no controls on the use of cryptography. In the vast majority of countries, cryptography may be freely used, manufactured, and sold without restriction. This is true for both leading industrial countries and for developing countries. There is a movement towards international relaxation of regulations relating to encryption products, coupled with a rejection of key escrow and recovery policies. Many countries have recently adopted policies expressly rejecting requirements for key escrow systems and a few countries, most notably France, have dropped their escrow systems. There are a small number of countries where strong domestic controls on the use of cryptography exist. These are mostly countries where human rights command little respect.

Recent trends in international law and policy point toward continued relaxation of controls on cryptography. The Organization for Economic Cooperation and Development's Cryptography Policy Guidelines and the Ministerial Declaration of the European Union, both released in 1997, argue for the liberalization of controls on cryptography and the development of market-based, user driven cryptography products and services. There is a growing awareness worldwide of encryption and an increasing number of countries have developed policies, driven by the OECD guidelines.

Export controls remain the most powerful obstacle to the development and free flow of encryption. The revised December 1998 Wassenaar Arrangement may roll back some of the liberalization sought by the OECD, particularly by restricting the key lengths of encryption products that can

Council Resolution of 1995 requires network operators and service providers to provide law enforcement agencies "in the clear" access to encrypted communications.[63]

12.2.10.22 The Commission is of the view that use should be made in clause 5A(1) of the term "capacity" and not "capability". The Commission is further of the view that the concerns of respondents on the issue of encryption should be dealt with in the suggested provision. The Commission considers that the provision should make it clear that a service provider will not be responsible to decrypt any encrypted communication unless such encryption forms part of the service concerned.

(c) Recommendation

12.2.10.23 The Commission recommends that clause 5A(1) provide that notwithstanding the provisions of any other law, no person, body or organization rendering a telecommunication

---

be exported without approval licenses. However, several major countries have already indicated that they do not plan to adopt new restrictions.

The United States government continues to lead efforts for encryption controls around the world. The US government has exerted economic and diplomatic pressure on other countries in an attempt to force them into adopting restrictive policies. The US position may be explained, in part, by the dominant role that national intelligence and federal law enforcement agencies hold in the development of encryption policy.

63 Ibid. The study *Data Protection and on-line Services: Regulatory Responses* conducted by Professors Joel R Reidenberg and Paul M Schwartz commissioned by the Directorate General XV of the Commission of the European Communities sets out the tension between cryptography and law enforcement concerns as follows:

One of the most controversial areas, at present, for the Internet and online services is the balance between cryptography and law enforcement concerns. On one hand, commercial services and individuals need and seek to improve the security of communications by using different kinds of cryptography for on-line transmissions of personal data, especially in the context of electronic payments.
The European Directive [95/46/EC art 17] requires the implementation of 'appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access'.
The European Directive further requires that such 'measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data protected' with due consideration of the state of the art and the cost of implementation. On the other hand, some law enforcement agencies in Europe argue that cryptography must be limited so police will be able to gain the access to online data necessary to fight organized crime. A debate that began in the United Sates concerning key escrow proposals and limits on the exportation of cryptography has been taken up through Europe. For example, the German Interior Minister has recently announced his key escrow proposal. Some German data protection commissioners are currently contesting his proposal's likely effectiveness. The European Commission has also taken a strong position in favor of the freedom of private parties to encrypt information.

service may provide any such service which does not have the capacity to be monitored; Provided that the person, body or organization rendering such a service shall not be responsible for decrypting any communication or conversation encrypted by the customer contracted for the use of the service, unless the facility for encryption was provided by the body, person or organization rendering the service.

12.2.11 Clause 5A(2): acquiring of facilities and devices at own cost from a supplier approved by the Minister for Posts, Telecommunications and Broadcasting[64]

(a) Comments on the proposed clause

12.2.11.1 MTN notes that the Commission proposes that the Minister responsible for Communications may issue a directive to state the period within which the necessary facilities and devices to enable monitoring of conversations must be operational. MTN states that this would provide the Minister responsible for Communications far more powers and jurisdiction than he has under the current Telecommunications Act. MTN notes that in terms of the Telecommunications Act such Minister has the power to issue directives relating to the policy that will be applied by the Government of the Republic of South Africa relating to telecommunications.

12.2.11.2 MTN also notes that this particular proposed section to the Monitoring Act also gives the Minister responsible for Communications the jurisdiction to approve suppliers from which the Network Operator should obtain certain facilities. MTN is of the view that this particular clause is inappropriate in that this would in essence give the Minister, as a political appointee, the power to influence the day to day operational requirements and decision making of a licenced telecommunications operator. MTN considers that by giving a political appointee the power to make decisions for and on behalf of a company goes against the grain of what is deemed to be commercial freedom in a democratic society. MTN also considers that this suggested clause read together with the proposed sub-clause 6 could have the effect of giving the Minister responsible for Communications a seat on the Board, a seat on the Executive Management of a telecommunication company as well as appoint such Minister as the

---

64 The term "Minister responsible for Communications" was used in the Bill contained in the discussion paper. The term used in the Telecommunications Act is "Minister for Posts, Telecommunication and Broadcasting" and it is therefore clear that this term should be applied.

Technical Officer of the telecommunications company. MTN is of the view that this again could surely not be the intention of the legislature.

12.2.11.3 MTN remarks it should further be noted that as the proposal currently reads, the Minister may issue such directive, with which MTN disagrees, without prior consultation, and could in effect approve a supplier whose equipment may not be compatible with the network of a Network Operator and even cause problems on the Network operated by the Network Operator.

12.2.11.4 Vodacom suggests that the Act should provide that the Minister may request that a type of service be provided, and that the provider shall make every reasonable attempt to make the service available. Vodacom suggests that this assumes that this Act will provide for "reasonable remuneration" for such facilities and services. Vodacom submits that the Minister should not dictate or approve the brand or type of equipment or supplier and that as long as the relevant service can be provided, these technical decisions - which could impact on the quality of operation of the network - should be left to the operator. Vodacom considers that the words "at own cost" and "from a supplier approved by the Minister responsible for Communications" should be deleted.

12.2.11.5 SATRA notes that this proposed amendment does not appear to be contentious. SATRA understands that the cost of acquiring such facilities would only be a small percentage of the total cost of the telecommunication service provided. SATRA considers that the cost of acquiring the facilities to monitor communications will, in any event, be passed onto the consumer whose interests are being protected by such a provision. SATRA states that in addition, if criminal elements are making use of the telecommunication service, provided then it should be incumbent upon the service provider to acquire the facilities to monitor illegal communications carried on its own lines of communication.

12.2.11.6 M-Web states that to the extent that the Discussion Paper states that the existing legislation in any event imposes the obligation on telecommunications services licensees to provide the necessary facilities and devices for monitoring and interception, regard should be had to the fact that this obligation was imposed when telecommunications services were provided by a, state-owned monopoly service provider. M-Web considers that the Act should be amended to ensure that only to the extent that a telecommunication services licensee

benefits from a State shareholding should it bear the obligation to pay the cost of the necessary facilities and devices. M-Web suggests that those licensees who do not benefit from a State "subsidy' should not be burdened with the cost. M-Web considers that in addition, whilst the precise detail is not to hand, preliminary investigations indicate that the cost of installing the necessary facilities and devices for monitoring and interception is very expensive as is the process of upgrading such facilities and devices to keep up with the pace of technological change. M-Web remarks that undermining the development of the industry in this way may amount to the imposition of an unreasonable means to achieve the end of combatting crime and may not be permitted in terms of constitutional review.

12.2.11.7 M-Web suggests that consideration should be given to the extent to which the proposed legislation imposes additional licence conditions on telecommunications services licensees which may expressly or impliedly conflict with the terms of the Telecommunications Act.

12.2.11.8 Globalstar SA remarks that it will, from the end of 1999, be the GMPCS (Global Mobile Personal Communications via Satellite) Country Operator for the Globalstar GMPCS system, as defined in a policy direction issued by the Minister of Post, Telecommunications and Broadcasting, in Government Gazette No. 19581, Vol. 402, dated 4 December 1998.[65] Globalstar notes that clause 6.7 of the Policy Direction states as follows:

> "The GMPCS service licensee shall comply with all applicable legislation, for example, the Interception and Monitoring Prohibition Act No. 127 of 1992."

12.2.11.9 Globalstar notes that as a public telecommunications service provider, Globalstar SA accepts that it has a public duty to assist the relevant authorities and agencies, as discussed in the paper, in being able to intercept and monitor telecommunications, where it is technically possible and feasible to do so. Globalstar says that where it is not currently technically possible and feasible to do so, there may be new technical developments required by telecommunications equipment manufacturers in order that an intercept and monitoring facility may be provided. Telecommunications service providers should therefore be given a reasonable period of time to introduce such a facility. Globalstar notes that the costs of

---

65 Policy Direction on global mobile personal communications by satellite in the Republic of South Africa. Issued by the Minister for Post, Telecommunications and Broadcasting in terms of section 5 of the Telecommunications Act 103 of 1996.

providing the technical facility for intercept and monitoring, and carrying out the activities associated with intercept and monitoring will be significant, and therefore it states it cannot agree to the recommendation at paragraph 11 (page x) of the Summary of Recommendations and Specific Requests for Comment which states that the remuneration payable to the telecommunications service provider "shall not include the costs of acquiring the facilities and devices referred to in section 5A(2)."

12.2.11.10 Globalstar states that providing a service on behalf of the state may be reasonable, but paying costs on behalf of the State is not reasonable in its view. Globalstar considers that this is particularly true of a relatively small niche market telecommunications service such as Globalstar SA, which will not command the large revenue associated with mass market services such as Telkom, Vodacom and MTN. Telecommunications service providers already pay taxes, licence fees, Universal Service fees, and/or contribute towards universal service in kind by providing community service telecommunications facilities in under-serviced areas all of which are beneficial to the State. Globalstar remarks that the proposed amendments to the Act impose yet another financial burden on the telecommunications service provider. They state that in summary, they support the principle of having an obligation to provide the ability for the Sate to carry out intercept and monitoring, if it is technically possible and feasible to do so, but all costs associated with providing the facility should be borne by the State.

12.2.11.11 Telkom considers that the obligation to acquire the facilities and devices within a stipulated time is problematic:

(a) The facilities and devices may not exist and will have to be developed for the purpose,
(a) Such persons as may be capable of providing or developing said facilities and devices may be persons subject to a foreign jurisdictions where the provision or supply of such may be restricted or prohibited.

12.2.11.12 Telkom also considers that the requirement that the Minister should approve the supplier is also problematic in this context: there might be only one supplier (e.g. the original equipment manufacturer, or the owner of an intellectual right) capable of supplying or developing the facilities or devices in question, making the Minister's approval meaningless, as his/her disapproval would prevent the service provider to fulfill the obligation imposed by this

subsection without providing relief. Telkom proposes that it is necessary that this subsection make provision for at least prior consultation with the service provider before any ministerial directive is issued. Telkom suggests that the Minister referred to in this section should be the same Minister referred to in section 5A(8). They further suggest the inclusion of the word 'interception' whenever the word 'monitoring' is used for the purpose of consistency. Telkom also states that the words 'from a supplier approved by the Minister responsible for Communications" should preferably be deleted. Telkom suggests that the Minister should not, and does not need to, have the power to prescribe the suppliers of telecommunications equipment.

12.2.11.13 Telkom considers that the clause as it is currently drafted, limits Telkom's commercial and contractual freedom. Telkom suggests the following amendment:

> Any person, body or organisation rendering a telecommunication service shall **[at own cost and within the period specified by the Minister responsible for Communications],** in accordance with a directive **[referred to]** issued in terms of subsection (6), acquire the necessary facilities and devices to enable the interception or monitoring of conversations and communications, of which the interception or monitoring has been authorised in terms of this Act, **[from a supplier approved by the Minister responsible for Communications].**

(b) Evaluation

12.2.11.14 The project committee considered that this clause harks back to what was said before about costs and that the only possible additional aspect is whether the clause should be retained or deleted. The committee notes that there is a concern from the service providers to being told what they should do and the facilities and devices to acquire. The committee considered the question whether clause 5A(1) read with subclause (2) caters for this situation and that it does not matter what equipment the service providers acquire, provided it has the capability/capacity to be monitored. The committee considered that the clause should be retained but resolved that the wording "of which the monitoring has been authorised in terms of this Act, from a supplier approved by the Minister responsible for Communications" should be deleted.

12.2.11.15 The Commission agrees with the approach and reasoning the project committee adopted in regard to this clause. The Commission concurs that the costs issue is at the heart

of the matter but notes that this aspect is presently being negotiated. The Commission notes the concerns of the telecommunication service providers being prescribed from which suppliers they should acquire the devices and facilities necessary to enable monitoring. The Commission is therefore also of the view that it does not matter what equipment the service providers acquire, provided it has the capacity to monitor. The Commission agrees with the project committee's proposal for the amendment of the clause.

(b) Recommendation

12.2.11.16 The Commission recommends that clause 5A(2) be retained but that the wording "of which the monitoring has been authorised in terms of this Act, from a supplier approved by the Minister responsible for Communications" should be deleted and recommends the following clause:

> Any person, body or organization rendering a telecommunication service shall at own cost and within the period specified by the Minister for Posts, Telecommunications and Broadcasting, in a directive referred to in subsection (6), acquire the necessary facilities and devices to enable the monitoring of conversations and communications.

12.2.12 Clause 5A(3): the investment, technical maintenance and operating costs in enabling a service to be monitored, shall be carried by the person, body or organization rendering the service

(a) Comments on the proposed clause

12.2.12.1 MTN suggests that clarity needs to be provided as to how the proposed Section 5(4) and Section 5A(3) should be read together. MTN notes that section 5(4) provides that remuneration only in respect of direct costs incurred in respect of personnel and administration shall be payable to a Network Operator whilst Section 5A(3) states that maintenance and operating costs shall be carried by the Network Operator. MTN suggets that similarly to their comments on Section 5(4), clarity needs to be provided so that Network Operators may be sure as to what costs it is envisaged may be carried by the Government.

12.2.12.2 SATRA states that the proposed provisions contained in paragraphs 14, 15, 16,

17 and 19 which seek to impose various obligations on telecommunication service providers to assist in monitoring communications are not problematic. SATRA considers that the propositions are in line with other countries with similar dispensations to South Africa. SATRA is satisfied that the judicial process will ensure that the rights of individuals are protected and that these rights will only be limited by interceptions and monitoring of communications when such limitation is reasonable and justifiable.

12.2.12.3 Telkom is of the view that this provision is both unreasonable and unfair. Telkom states that it is unreasonable because while capability and capacity required are determined by the security entities, the cost is born by the service provider. As the security entities do not bear the costs, they have no incentive to confine their requirements to what is necessary and reasonable, nor is there any provision in the Act to compel them to do so. The service provider, on the other hand has no way to resist unreasonable requests. Telkom considers it is unfair because it puts the burden of financing an activity of the state, security and crime prevention, on a predetermined section of the population, the providers of telecommunication services and through them their customers. They state that with respect to Telkom it is also unfair because it creates what could be extremely onerous financial obligations, which were not taken into account when Telkom committed itself to the roll-out obligations in its PSTS licence. Telkom considers that the problem is further exacerbated by the fact that Telkom, unlike other telecommunication service providers, is subject to a Price Cap regime in its licence which restricts its ability to recover these costs from its other customers.

12.2.12.4 Telkom notes that the Commission relies on the approach adopted in the Netherlands as precedent for this provision. Telkom states that the Commission does not, however, provide any details of any safeguards, reasonableness requirements or any other circumstances that may temper the financial burden of the telecommunication service providers. Telkom considers that if the cost quoted with regard to the provisions of such services in the USA of between $500 million and $1.8 billion can be of any assistance, it should be evident that the proposed amendment may result in Telkom being unable to meet its roll-out obligations, which would entitle Telkom to invoke the limitation provisions of condition 1 3.4.2 of its PSTS licence. Telkom suggests that maintenance costs and costs pertaining to the upgrading of the software with regard to this equipment, should also be considered.

12.2.12.5 Vodacom considers that the costs to the procurement of the monitoring and

interception equipment, as well as the provision of the facilities and services, should be borne by the State and must be paid for from the *fiscus*. Vodacom is of the view that the imposition of this condition would constitute an amendment to existing licenses and that any amendment to the terms and conditions of existing licenses should be effected in terms of the Telecommunications Act.

(b) Evaluation

12.2.12.6 The project committee addressed this aspect above when it stated that there are two opposing views on the question who should bear the costs involved in enabling a telecommunication service to be monitored, and that it considered these costs should be borne by telecommunication service providers. The committee therefore considered that the clause should not be amended.

12.2.12.7 The Commission agrees with the project committee and considers that the telecommunication service providers should bear the investment, technical, maintenance and operating costs in enabling a telecommunication service to be monitored.

(c) Recommendation

12.2.12.8 The Commission recommends that clause 5A(3) should provide that the investment, technical, maintenance and operating costs in enabling a telecommunication service to be monitored, should be carried by the person, body or organisation rendering such a service.

12.2.13 Clause 5A(4): routing of duplicate signals to relevant central monitoring centre

(a) Comments on the proposed clause

12.2.13.1 Telkom states that save for what said above in respect of costs, forecasting of capacity, and possible complexity in accessing the signal to be duplicated, this provision seems acceptable. Vodacom suggests that the clause should provide that the telecommunication service operator shall make the necessary connections to ensure that duplicate signals of conversations and communications authorised to be monitored in terms of the Act are capable

of being routed to the relevant central monitoring centre, to be designated by, respectively, the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force, and the Directors-General of the Agency and Service.[66] Vodacom explains that a network operator should not be expected to play any role in the monitoring and interception exercise save the making available of the appropriate connections for the monitoring (including the recording and play back) devices to the appropriate State agency, which should be carried out by the relevant State agency. Vodacom suggests that the State agency concerned must carry the full responsibility for the storage or archiving of the recordings and for taking all steps as are reasonably necessary for the verification of its authenticity. Vodacom considers that the telecommunication service operator should simply make a "*connection*" and not monitor with whom the monitored party is speaking.

12.2.13.2 The Law Society of SA's standing committee on constitutional affairs considers that it is unclear from the wording of this clause, who would be responsible for the costs incurred in the relaying of duplicate conversations and communications in terms of the Act.

(b) Evaluation

12.2.13.3 It is clear that the proposed clause does not impose the duties Vodacom considers it to impose on telecommunication service operators such as storage or archiving of recordings. Save for the Vodacom's concerns and those of the Law Society of South Africa about the cost aspect involved in routing duplicate signals, the suggested clause did not lead to opposition. The Commission is of the view that there is no need to set out in more detail what the role and duties of telecommunication service operators are in routing duplicate signals to the proposed central monitoring centre. The Commission is therefore of the view that the proposed clause should be retained in the Bill.

(c) Recommendation

---

66 The proposed clause 5A(4) contained in the discussion paper provided as follows:
(4) Duplicate signals of conversations and communications authorized to be monitored in terms of this Act, shall be routed by the relevant person, body or organization rendering a telecommunication service to the relevant central monitoring centre, to be designated by, respectively, the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force, and the Directors-General of the Agency and Service.

12.2.13.4 The Commission recommends that the Bill should provide that duplicate signals of conversations and communications authorized to be monitored in terms of this Act, shall be routed by the relevant person, body or organization rendering a telecommunication service to the relevant central monitoring centre, to be designated by, respectively, the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force, and the Directors-General of the Agency and Service.

12.2.14 Clause 5A(5): central monitoring centres to be equipped and maintained at State expense

(a) Comments on the proposed clause

12.2.14.1 Telkom suggests that the proposed text should be amended as follows: "...at State expense, equip, operate and maintain central monitoring centres ... Telkom considers that it should be made clear that the telecommunication service provider is in no way responsible for costs, including the operating costs, incurred in relation to the central monitoring centre and the recording equipment associated with it. Telkom notes that the location and amount of monitoring centers will have an effect on the cost and may need an expansion on our network. Telkom suggests that clause 5A(5) be amended as follows:

> The South African Police Service, the South African National Defence Force, the Agency and the Service shall, at State expense, equip, operate and maintain central monitoring centres for the authorised monitoring of conversations or communications: Provided that an agreement on the sharing of any such central monitoring centre shall not be excluded.

(b) Evaluation

12.2.14.2 The project committee noted that when it met with representatives of the Intelligence community and the telecommunication service providers that the intention of the three agencies mentioned in the clause seems to be that central monitoring centres for the authorised monitoring of conversations or communications will be will be equipped, operated and maintained at State expense. The project committee did not have a specific view on this aspect but it seems to the Commission that it may be useful to include the phrase "operate" in the clause as suggested by Telkom.

(c) Recommendation

12.2.14.3 The Commission recommends that clause 5A(5) be amended by the insertion of the word "operate" in the clause to read as follows:

> The South African Police Service, the South African National Defence Force, the Agency and the Service shall, at State expense, equip, operate and maintain central monitoring centres for the authorised monitoring of conversations or communications.

12.2.15 Clause 5A(6): the Minister may issue a directive to comply with his or her directive specifying the security, technical and functional requirements of facilities and devices

(a) Comments on the proposed clause

12.2.15.1 Telkom considers that this clause seems to give the Minister the discretion to determine who must comply with subsection 5A(1). Telkom notes that the latter, however, creates an obligation applicable to all providers of telecommunication services. Telkom suggests that the Minister referred to in this section should be the same minister referred to in section 5A(8). Telkom remarks that since non-compliance with a directive can lead to the revoking of a telecommunication licence, it would be advisable that the Minister consults with the telecommunication service/network providers before any directive is issued. Telkom considers that consultation would allow the telecommunication service/network providers the opportunity to advise the Minister as to the technical and operational nature and limitations of their networks. Telkom suggests amending the clause as follows:

> The Minister **[responsible for Communications]** for Posts, Telecommunications and Broadcasting **[may]** shall after consultation with [issue a directive to] any person, body or organisation rendering a telecommunication service, issue a directive to comply with subsection (1) and may, in such direction, specify the security, technical and functional requirements of the facilities and devices to be acquired in terms of subsection (2).

12.2.15.2 MTN considers that this particular section is unreasonable. MTN notes that the Minister responsible for Communication in terms of the Telecommunications Act may issue directives relating to policy. MTN remarks that the proposed directives that the Minister responsible for Communications is capable of issuing may specify the security, technical and

functional requirements of the facilities and devices to be acquired to do the necessary monitoring of conversations or communications. MTN states that similarly to their comments on Section 5A(2) such Minister would therefore be able to interfere with the commercial freedom of a Licenced Telecommunications Network Operator. MTN considers that such Minister would therefore also be able to interfere with whatever contractual arrangements such Network Operator may have with suppliers.

12.2.15.3 In MTN's view this particular method of requiring Network Operator's to do or purchase equipment from a certain supplier with certain technical and functional requirements is an amendment to the Licences granted to the a Telecommunications Network Operator without following the processes and procedures as contained in either the Telecommunications Act or the various Licences granted to Network Operators. It is therefore MTN's opinion that the inclusion of such a section is unreasonable and inappropriate. M-Web states that clause 5B(6) appears to be too wide in its application both in terms of the information that may be requested and the basis upon which such information may be requested.

12.2.15.4 Vodacom notes that should it prove necessary to require the provisioning of such facilities under clauses 5(6) and (7) of the Bill, then the Minister should be required to follow an appropriate administrative law procedure including a hearing with the affected parties and obtaining their agreement where necessary. Vodacom proposes the following clause 5A(6):

> The Minister responsible for Communications may, after consultation with, or where necessary, obtaining the agreement of the relevant person, body or organisation, issue a directive to any person, body or organisation rendering a telecommunication service, to comply with subsection (2) and may, in such direction, specify the security, technical and functional requirements of the facilities and devices to be acquired in terms of subsection (2) and such person, body or organisation shall make every reasonable attempt to make the service available.

(b) Evaluation

12.2.15.5 The project committee was of the view that the Minister should be required to consult with the parties concerned. The question arose whether the clause should provide that the Minister may issue the directive concerned "after consultation" or "in consultation" with the parties concerned. The committee noted that if the clause makes provision for "in consultation" one of the parties has a veto. The committee resolved that the clause should be amended to read "The Minister for Posts, Telecommunications and Broadcasting, after consultation with any

person, body or organisation rendering a telecommunication service, may issue a directive to comply with subsection (1) ...". The committee also resolved that the word "direction" should throughout the Bill be replaced with the term "directive". The committee notes that there was also objection to the Minister specifying the security, technical and functional requirements of facilities and devices to be acquired. The committee was of the view that the Minister should be empowered by the Act to specify that the facilities and devices should be of a certain standard.

12.2.15.6 The Commission agrees with the project committee that the Bill should make provision for the Minister for Posts, Telecommunications and Broadcasting consulting with the parties concerned and that the Minister should be able to specify the security, technical and functional requirements of the facilities and devices to be acquired by a person, body or organisation rendering a telecommunication service.

(c) Recommendation

12.2.15.7 The Commission recommends that the Bill should provide that the Minister for Posts, Telecommunications and Broadcasting after consultation with any person, body or organisation rendering a telecommunication service, may issue a directive to comply with section 5A(1) and may, in such directive, specify the security, technical and functional requirements of the facilities and devices to be acquired by a person, body or organisation rendering a telecommunication service.

12.2.16 Clause 5A(7): capacity, systems used, connectivity, etc

(a) Comments on the proposed clause

12.2.16.1 MTN states that similarly to Sub-clause 6, Sub-clause 7 as proposed gives the Minister responsible for Communications the power to specify matters such as capacity, systems to be used and connectivity. MTN points out that the current wording of the suggested Sub-clause 7, seems to indicate that it will be the obligation of the Network Provider to ensure the connectivity with the designated central monitoring centres. MTN considers that this would entail that in an instance where the systems of the Network Operator cannot connect with, or in other words, handshake with the systems of the Central Monitoring System, the Network

Operator may fall foul of this obligation in that it would not be able to provide such connectivity.

12.2.16.2 Telkom states that it is doubtful whether the Minister will in fact have the capability to specify some of the listed elements, as often only the affected service provider, or the equipment supplier, will have the required technical information. Telkom notes that there is no obligation on the Minister to consult with the affected party before a ministerial directive is issued. Telkom considers that its proposed amendments to section 5A(5) would address these issues.

12.2.16.3 M-Webb notes that the provisions of this clause may be too wide in their scope and may be virtually impossible to implement in respect of pre-paid subscribers to some services.

(b) Evaluation

12.2.16.4 The project committee was of the view that since it considered that the Bill should require the Minister to consult with all the parties involved in rendering telecommunication services, the proposed provision is appropriate. The Commission is of the view that the provision as proposed by the project committee is appropriate, particularly once provision is made for the Minister to consult with the relevant parties.

(c) Recommendation

12.2.16.5 The Commission recommends that the Bill should provide that the directives issued by the Minister referred to in subsection (6) may include, but are not limited, to specifications on the following -

(a) the capacity needed for interception purposes;
(b) systems to be used;
(c) connectivity with designated central monitoring centres;
(d) the manner of transmission of duplicated signals of conversations and communications to be intercepted, to the designated central monitoring centres referred to in subsection (5); or
(e) the manner of transmission of call-related data to the central monitoring centres, referred to in section 5B.

12.2.17 Clause 5A(8): period of three months to comply with directive

(a) Comments on the proposed clause

12.2.17.1 Telkom notes that the clause makes no provision for consultation. Telkom suggests the clause to be amended as follows:

> The Minister for Posts, Telecommunications and Broadcasting may after consultation with the person, body or organisation rendering the telecommunication service determine a period, which shall not be less than three months from the date on which a direction in terms of subsection (6) is issued, for compliance with such a direction.

12.2.17.2 MTN considers that the time period referred to in Sub-Section 8, which shall not be less than three months, does not take into regard the realities of telecommunications. MTN suggests that proper investigation as well as configuration of new systems in a Network such as the Network operated by MTN could mean that such systems as specified by the Minister might not be able to be integrated into the Network operating systems of MTN. MTN states that in such an instance MTN would be deemed to be in breach of a directive, and on the reading of the proposed Bill, in breach of a Licence. MTN suggests that again such must be seen as an amendment to the current Licence of MTN without going through the proper processes and procedures as envisaged in the Telecommunications Act and the various Licences granted to MTN.

(b) Evaluation

12.2.17.3 The project committee took into account the suggestion by Telkom that consultation should also be required in this instance. The committee resolved that consultation should be required here as well as there are drastic consequences for non-compliance. The committee resolves that the clause be amended to read "the Minister for Posts, Telecommunications and Broadcasting may, after consultation with the person, body or organisation concerned rendering a telecommunication service, determine a period, which shall not be less than three months from the date ...".

12.2.17.4 The Commission is also of the view that Telkom's suggestion on the Minister having to consult in terms of this provision is persuasive.

(c) Recommendation

12.2.17.5 The Commission recommends that clause 5A(8) provide that the Minister for Posts, Telecommunications and Broadcasting may after consultation with the person, body or organisation rendering the telecommunication service, determine a period, which shall not be less than three months from the date on which a directive in terms of subsection (6) is issued, for compliance with such a directive.

12.2.18 Clause 5B(1): provision of call-related information on an ongoing basis for a specified duration and clause 5B(2): routing the information to the designated central monitoring centre

(a) Comment on the proposed clause

12.2.18.1 MTN considers that it is clearly the intention of the proposal that Network Operators become Agencies of the various Security Structures of the Government to provide such surveillance as may be contained in a directive issue by a Judge. MTN points out that if not Sub-clause 1, then Sub-clause 3 clearly indicates that Network Operators will become Agencies for and on behalf of the Police and other Security Structure for surveillance and "agtervolging" of the target, in that call-related data, which includes the position of the person being tracked, needs to be divulged to such structures.

12.2.18.2 Telkom considers that the meaning of the term 'on an ongoing basis" is not clear. Telkom states that it presumes that 'on an on-going basis' will mean for the duration of the direction. Telkom notes that this subsection provides that call-related data associated with a conversation or communication to be monitored can also be requested by the monitoring entity from a judge. Telkom states that the provision of such data by the telecommunication service/network provider, should therefore be subject to the same terms and conditions as are applicable to the monitoring of calls. Telkom therefor proposes the following amendment:

> Any person who is authorized to apply for a direction referred to in section 2(2), may also apply, in the manner prescribed in this Act for the application for a direction for interception or monitoring, for the provisioning **[on an ongoing basis]** of call-related data relating to the conversations or communications mentioned in the direction, and the judge may authorize such provisioning in the same direction.

12.2.18.3 The NICOC subcommittee proposes that the words "on an ongoing basis" should be qualified by the insertion of the words "for the duration of the direction, as it becomes available".

(b) Evaluation

12.2.18.4 The project committee noted the proposal that the provision of call-related information "on an ongoing basis" should be qualified by the addition of the words "for the duration of the directive, as it becomes available". The committee considered that the clause makes provision for two directives, namely a main directive authorising interception of communications or conversations and a subsidiary directive authorising the provision of call-related information. The committee was of the view that the suggestion for amending the clause is persuasive. The committee considered that what the clause seeks to provide is that the person who is entitled to apply for a directive may also apply for a directive authorising the provision of call-related information, hence, the person who may apply under section 2(2) of the Act for an interception, may also apply for a directive for call-related information. The committee argued that obviously if one has already made or is busy making contemporaneously an application for monitoring, then the application for call-related information is for an additional form of relief.

12.2.18.5 The committee resolved that the clause should be amended to read as follows: "Any person who is authorised to apply for a directive in terms of section 2(2), may also apply, in the manner prescribed in this Act, for a directive for the provision on an ongoing basis for the duration of the directive, as it becomes available, of call-related information". The committee was of the view that there is no need for the retention in the clause of the proposed words "relating to the conversations or communications mentioned in the direction, and the judge may authorize such provisioning in the same direction".

12.2.18.6 The project committee noted that clause 5B(2) seeks to provide that any person, body or organization rendering a telecommunication service shall, in respect of all conversations or communications which are monitored in terms of this Act, route the call-related information specified in a directive referred to in subsection (1) and section 2(2), to the relevant designated central monitoring centre. The project committee was of the view that apart from the phrase "call-related data" which should be substituted with the phrase " call-related

information" and the term "direction" with the term "directive", the wording of clause 5B(2) is appropriate.

12.2.18.7 The Commission is of the view that clause 5B(1) should make provision for any person who is authorised to apply for a directive to also apply for a supplementary directive for the provision on an ongoing basis for a specified duration of call-related information as it becomes available. The Commission concurs with the opinion of the project committee that there is no need to retain the phrase "relating to the conversations or communications mentioned in the direction, and the judge may authorize such provisioning in the same direction". The Commission has, furthermore, no objections to the proposed clause 5B(2).

(c) Recommendation

12.2.18.8 The Commission recommends that clause 5B(1) provide that any person who is authorised to apply for a directive in terms of section 2(2), may also apply, in the manner prescribed in the Act, for a supplementary directive for the provision on an ongoing basis for a specific duration of call-related information, as it becomes available.

12.2.18.9 The Commission also recommends the insertion of a clause 5B(2) in the Bill making provision that any person, body or organization rendering a telecommunication service must route the call-related information specified in a supplementary directive to the relevant designated central monitoring centre.

12.2.19 Clause 5B(3): judge may direct the provision of call-related information on an ongoing basis

(a) Comments on the proposed clause

12.2.19.1 Telkom considers that again, the words "on an ongoing basis" should be deleted for reasons stated in respect of clause 5B(1) above. Telkom notes that while it is clear that this subsection intends to provide for the monitoring of call data only, it is not clear why the last sentence "... for purposes relating to the functions .. ' is used. Telkom is of the view that these words should be deleted and substituted with "for purposes of this Act". Telkom proposes the following amendment:

If, in a specific case, only call-related data is required **[on an ongoing basis]** without the actual monitoring of the conversation or communication in question, the judge may direct that the relevant person, body or organisation rendering a telecommunication service to whom or which a direction is addressed, provide such call-related data **[for purposes relating to the functions of the South African Police Service, the South African National Defence Force, the Agency or the Service, whatever is applicable]** for the purposes of this Act.

12.2.19.2 M-Web notes that generally the provisions of the proposed Section 5B(3) are not clear, for example what is envisaged by the collection of "... call-related data.... on an ongoing basis without the actual monitoring of the conversation or communication in question...".

12.2.19.3 Judge Gordon remarks that granting an order on an "ongoing basis" does not appear to him to be advisable. Vodacom considers that the provisioning of call-related information (particularly with location data) without monitoring or intercepting constitutes surveillance. Vodacom therefore suggests that the Act should explicitly state that the purpose is "*surveillance*" and not the interception and or monitoring of a communication. Vodacom considers that if this is not achievable in this amendment Bill, the clause must be deleted. Vodacom remarks that it would support specific clauses or a specific piece of legislation which would require judicial oversight of such electronic surveillance activities.

12.2.19.4 The NICOC subcommittee considers that clause 5B(3) should be amended to read as follows: "If, in a specific case, only call-related data is required on an ongoing basis **[without the]** regardless of any monitoring of the conversation ...."

(b) Evaluation

12.2.19.5 The project committee considered whether the clause should be further amended by providing in the clause that the call-related information should be routed to the relevant designated central monitoring centre as referred to in subsection (2) and hence the substitution of the words "the South African Police Service, the South African National Defence Force, the Agency or the Service, whatever is applicable with "the central monitoring centre referred to in subsection(2)". The committee notes that this might not be technically correct since the committee was advised that the information goes to the party requesting the information. Therefore, absent a directive by the judge to whom the information should go, it goes to the

party requesting the information. The committee notes however that one party such as the National Intelligence Agency may for example apply for a directive. There may be a serious security issue at hand and NIA applies that the calls of a suspect be monitored. Although only the Agency applies, it may be a joint operation of the Police Services and the Defence Force and the parties concerned may wish the information to be supplied to the Police and Defence Force as well, and the judge has then to direct the distribution of the information. The project committee resolved that there does not seem to be a prohibition against such a distribution of information. The committee further noted the concerns against the wording "for purposes relating to the functions of" the SA Police Service, the SA National Defence Force, the Agency and the Service and decided that there is no need for the retention of these words.

12.2.19.6 The Commission agrees with the project committee on the deletion of the words "for purposes relating to the functions of" and considers that the remainder of the proposed clause is appropriate.

(c) Recommendation

12.2.19.7 The Commission recommends that clause 5B(3) should read as follows:

> If, in a specific case, only call-related information is required on an ongoing basis without the actual monitoring of the conversation or communication in question, the judge may direct that the relevant person, body or organisation rendering a telecommunication service to whom or which a directive is addressed, provide such call-related information to the South African Police Service, the South African National Defence Force, the Agency or the Service, whichever is applicable.

12.2.20 Clause 5B(4): the provisions of the Act on the provision of call-related information excludes the use of any power in any other Act to obtain evidence or information in respect of a person, body or organisation

(a) Comments on the proposed clause

12.2.20.1 Vodacom remarks that the level of intrusion that can be achieved by utilising mobile cellular technology can be very high and should in such case require judicial oversight. Vodacom considers that it would therefore be administratively preferable and more consonant with constitutional principles, if all requests for ongoing "*real time*" call-related information

(which includes location information) were expressly brought under this or a separate piece of legislation by treating "*electronic surveillance*" as a specific category of enforcement activity.

(b) Evaluation

12.2.20.2 The project committee was of the view that the proposed clause should be retained in the Amendment Act. The committee noted that law enforcement agencies may make use of the provisions of section 205 of the Criminal Procedure Act and section 11 of the Drugs and Drug Trafficking Act, 1992 to presently obtain call-related information.

12.2.20.3 The Commission notes that the Criminal Procedure Act of 1977 and the Drugs and Drug Trafficking Act of 1992 confers powers on law enforcement agencies to obtain evidence such as call-related information. The Commission poses the question whether this situation should be sanctioned by the proposed clause 5B(4) and whether the Interception Act should permit certain agencies to request the provision of call-related information. The question as to abuse of the provisions arises and whether these Acts contain sufficient safeguards justifying the provision of call-related information under these or other laws.

12.2.20.3 The Commission is of the view that the case of *Malone v United Kingdom* heard by the European Court for Human Rights should be considered in this regard. The court remarked as follows on the furnishing of call-related information to the police and the absence of legal provisions concerning the scope and manner of exercise of the discretion enjoyed by the public authorities to comply with a request from the police to make and supply records of "metering" or call-related information.

> The process known as 'metering' involves the use of a device (a meter check printer) which registers the numbers dialled on a particular telephone and the time and duration of each call (see paragraph 56 above). In making such records, the Post Office - now British Telecommunications - makes use only of signals sent to itself as the provider of the telephone service and does not monitor or intercept telephone conversations at all. From this, the Government drew the conclusion that metering, in contrast to interception of communications, does not entail interference with any right guaranteed by Article 8 (art. 8).
>
> As the Government rightly suggested, a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service.

By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8 (art. 8). The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 (art. 8).

As was noted in the Commission's decision declaring Mr. Malone's application admissible, his complaints regarding metering are closely connected with his complaints regarding interception of communications. The issue before the Court for decision under this head is similarly limited to the supply of records of metering to the police "within the general context of a criminal investigation, together with the legal and administrative framework relevant [thereto]" (see paragraph 63 above).

In England and Wales, although the police do not have any power, in the absence of a subpoena, to compel the production of records of metering, a practice exists whereby the Post Office do on occasions make and provide such records at the request of the police if the information is essential to police enquiries in relation to serious crime and cannot be obtained from other sources (see paragraph 56 above). The applicant, as a suspected receiver of stolen goods, was, it may be presumed, a member of a class of persons potentially liable to be directly affected by this practice. The applicant can therefore claim, for the purposes of Article 25(art. 25) of the Convention, to be a "victim" of a violation of Article 8 (art. 8) by reason of the very existence of this practice, quite apart from any concrete measure of implementation taken against him (cf., mutatis mutandis, paragraph 64 above). This remains so despite the clarification by the Government that in fact the police had neither caused his telephone to be metered nor undertaken any search operations on the basis of any list of telephone numbers obtained from metering (see paragraph 17 above; see also, mutatis mutandis, the above-mentioned Klass and Others judgment, Series Ano. 28, p. 20, para. 37 in fine).

Section 80 of the Post Office Act 1969 has never been applied so as to 'require' the Post Office, pursuant to a warrant of the Secretary of State, to make available to the police in connection withthe investigation of crime information obtained from metering. On the other hand, no rule of domestic law makes it unlawful for the PostOffice voluntarily to comply with a request from the police to make and supply records of metering (see paragraph 56 above). The practice described above, including the limitative conditions as to when the information may be provided, has been made public in answer to parliamentary questions (ibid.). However, on the evidence adduced before the Court, apart from the simple absence of prohibition, there would appear to be no legal rules concerning the scope and manner of exercise of the discretion enjoyed by the

public authorities. Consequently, although lawful in terms of domestic law, the interference resulting from the existence of the practice in question was not 'in accordance with the law', within the meaning of paragraph 2 of Article 8 (art. 8-2) (see paragraphs 66 to 68 above).

This conclusion removes the need for the Court to determine whether the interference found was "necessary in a democratic society"for one of the aims enumerated in paragraph 2 of Article 8(art. 8-2) (see, mutatis mutandis, paragraph 82 above).

12.2.20.4 Vodacom mentions that the level of intrusion that can be achieved by utilising mobile cellular technology can be very high. In *R v Wise*[67] the Canadian Supreme Court considered the intrusion caused by the monitoring of a vehicle when use is made of tracking devices. The majority and dissenting views of the court were as follows:

- The installation of the beeper inside the appellant's vehicle constituted an unreasonable search in violation of s. 8 of the *Charter*. Since the subsequent monitoring of the vehicle invaded a reasonable expectation of privacy, it also constituted a search, and, in the absence of prior authorization, violated s. 8. The search was only minimally intrusive, however. The expectation of privacy in a motor vehicle is much less than in one's home or office. As well, the device used was unsophisticated and inaccurate. It was a very rudimentary extension of physical surveillance, and was attached to the appellant's vehicle, not to the appellant. The police also had a bona fide belief that they were protecting the public when the device was installed, in view of the series of homicides in the rural area in which the appellant lived.

  The admission of the evidence in this case would not bring the administration of justice into disrepute. The evidence as to the location of the car would not affect the fairness of the trial. This evidence was real, not conscriptive. There was no police compulsion or enticement which required appellant to enter or drive his car. The beeper merely helped the police to gather evidence which, to a great extent, they had obtained by visually observing the vehicle. The police also acted in good faith in this case. They had reasonable and probable grounds for searching appellant's vehicle when they installed the beeper. While the prolonged electronic monitoring after the metal filings were discovered is difficult to justify, the police obtained the evidence as to the location of the vehicle within a 30-day period, and this was not an unreasonable length of time to maintain surveillance, particularly in light of their obligation to protect the community from the suspected serial killer. There was clearly a pervasive threat of violence and a sense of urgency here. Moreover, the offence in this case is a serious one. The evidence pertaining to the metal pieces should also be admitted, for the same reasons.[68]

- The installation of the tracking device in appellant's car constituted an unlawful trespass and violates his privacy rights under s. 8 of the *Charter*. The use of the device to monitor his movements also violated s. 8. An individual has a reasonable expectation of privacy not only in the communications he makes, but in his movements as well, even when travelling on a public road. This is not a case where the police are monitoring the roads for the purpose of regulating or observing what goes on there. It is a case of tracking the movements of an individual. There is an important difference between courting the risk that our activities may be observed by other persons and the risk that agents of the state, in the absence of prior authorization, will track our

---

67 *R. v. Wise* [1992] 1 S.C.R. 527.

68 *Per* Lamer C.J. and Gonthier, Cory and Stevenson JJ.

every move. It is constitutionally unacceptable that the state should be allowed to rest a justification for the unauthorized electronic surveillance of a given person on the mere fact that that person had been in a situation where he could be the object of scrutiny on the part of private individuals. Whether a person whose movements were surreptitiously tracked had a reasonable expectation of privacy in given circumstances must not be made to depend on the degree to which that person took measures to shield his or her activities from the scrutiny of other persons.[69]

The grave threat to individual privacy posed by surreptitious electronic tracking of one's movement is such as to require prior judicial authorization. The issuance of a search warrant will ordinarily call for an objective showing of reasonable and probable cause, and this should generally be required of those seeking to employ electronic tracking devices in the pursuit of an individual. Since this means of surveillance, if properly controlled, is somewhat less intrusive than electronic audio or video surveillance, it may be possible to establish that judicial officers should be empowered in certain circumstances to accept a somewhat lower standard, such as a "solid ground" for suspicion, if it can be established that such a power is necessary for the control of certain types of dangerous or pernicious crimes.

The evidence obtained through the use of the tracking device should be excluded under s. 24(2) of the *Charter*. Such evidence would not have existed without the device because visual contact had been lost. Since the violation in this case was intrusive and long-lasting, it was serious. The electronic surveillance continued day and night over many months. The violation was not mitigated by good faith on the part of the police. The police certainly knew they needed a warrant to search the car, and that the warrant they had obtained did not permit what they did, and in fact had expired. The police did not have reasonable and probable cause, but were acting on mere suspicion. The long-term consequences of admitting evidence obtained in such circumstances on the integrity of our justice system outweigh the harm done by this accused being acquitted.

12.2.20.5 The Commission has noted the requirements posed by the Criminal Procedure Act and the Drug and Drugs Trafficking Act. These Acts set out the procedure how police officials must apply for warrants if they wish to obtain information. The issue is whether these provisions are adequate. In the case of the Criminal Procedure Act[70], law enforcement

---

69 *Per* La Forest J. (dissenting).

70 (1) A judge of the Supreme Court, a regional court magistrate or a magistrate may, subject to the provisions of subsection 4, upon the request of an attorney-general or a public prosecutor authorized thereto in writing by the attorney-general, require the attendance before him or any other judge, regional court magistrate or magistrate, for examination by the attorney-general or the public prosecutor authorized thereto in writing by the attorney-general, of any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the attorney-general or public prosecutor concerned prior to the date on which he is required to appear before a judge, regional court magistrate or magistrate, he shall be under no further obligation to appear before a judge, regional court magistrate or magistrate.
(2) The provisions of sections 162 to 165 inclusive, 179 to 181 inclusive, 187 to 189 inclusive, 191 and 204 shall mutatis mutandis apply with reference to the proceedings under subsection (1).
(3) The examination of any person under subsection (1) may be conducted in private at any place designated by the judge, regional court magistrate or magistrate.
(4) A person required in terms of subsection (1) to appear before a judge, a regional court

agencies have to submit affidavits setting out to State Prosecutors or Directors of Public Prosecution the grounds for the attendance of the person concerned before a Judge, Magistrate or Regional Court Magistrate. The affidavit is not submitted to the Judge, Magistrate or Regional Court Magistrate who decides whether or not the person concerned should be required to appear before him or her. It is therefore clear that the requirements of the Criminal Procedure Act does not contain the same degree of safeguards which the proposed Bill contains on satisfying a judge to grant a directive for the provision for call-related information.

The Drug and Drugs Trafficking Act[71]

---

magistrate or a magistrate for examination, and who refuses or fails to give the information contemplated in subsection (1), shall not be sentenced to imprisonment as contemplated in section 189 unless the judge, regional court magistrate or magistrate concerned, as the case may be, is also of the opinion that the furnishing of such information is necessary for the administration of justice or the maintenance of law and order.

71 11(1) A police official may-

(a) if he has reasonable grounds to suspect that an offence under this Act has been or is about to be committed by means or in respect of any scheduled substance, drug or property, at any time-

(i) enter or board and search any premises, vehicle, vessel or aircraft on or in which any such substance, drug or property is suspected to be found;

(ii) search any container or other thing in which any such substance, drug or property is suspected to be found;

(b) if he has reasonable grounds to suspect that any person has committed or is about to commit an offence under this Act by means or in respect of any scheduled substance, drug or property, search or cause to be searched any such person or anything in his possession or custody or under his control: Provided that a woman shall be searched by a woman only;

(c) if he has reasonable grounds to suspect that any article which has been or is being transmitted through the post contains any scheduled substance, drug or property by means or in respect of which an offence under this Act has been committed, notwithstanding anything to the contrary in any law contained, intercept or cause to be intercepted either during transit or otherwise any such article, and open and examine it in the presence of any suitable person;

(d) question any person who in his opinion may be capable of furnishing any information as to any offence or alleged offence under this Act;

(e) require from any person who has in his possession or custody or under his control any register, record or other document which in the opinion of the police official may have a bearing on any offence or alleged offence under this Act, to deliver to him then and there, or to submit to him at such time and place as may be determined by the police official, any such register, record or document;

(f) examine any such register, record or document or make an extract therefrom or a copy thereof, and require from any person an explanation of an entry in any such register, record or document;

(g) seize anything which in his opinion is connected with, or may provide proof of, a contravention of a provision of this Act.

(2) A police official may in the exercise of his powers under this section-

(a) require any vehicle, vessel or aircraft to be stopped; or

(b) request the master, pilot or owner of any vessel or aircraft to sail or to fly any such vessel or aircraft, or to cause it to be sailed or flown, to such harbour or airport as may be

requires that any person who has in his or her possession, custody or control any register, record or other document which in the opinion of the police official may have a bearing on any offence or alleged offence under the Act, to deliver to the official concerned then and there, or

---

indicated by the police official.

12(1) Whenever it appears to a magistrate from information submitted to him on oath by the attorney-general concerned, or by any public prosecutor authorized thereto in writing by that attorney-general, that there are reasonable grounds for believing that any person is withholding any information as to a drug offence, whether the drug offence has been or is being or is likely to be committed in the Republic or elsewhere, from that attorney-general, any such public prosecutor or any police official, as the case may be, he may issue a warrant for the arrest and detention of any such person.

(2) Notwithstanding anything to the contrary in any law contained, any person arrested by virtue of a warrant under subsection (1) shall as soon as possible be taken to the place mentioned in the warrant and detained there, or at such other place as the magistrate may from time to time determine, for interrogation in accordance with the directions, if any, issued by the magistrate from time to time.

(3) Any person arrested and detained under a warrant referred to in subsection (1) shall be detained until the magistrate orders his release when satisfied that the detainee has satisfactorily replied to all questions at the interrogation or that no useful purpose will be served by his further detention: Provided that the attorney-general concerned may at any time direct in writing that the interrogation of any particular detainee be discontinued, whereupon that detainee shall be released without delay.

(4)(a) Any person arrested under a warrant referred to in subsection (1) shall be brought before the magistrate within 48 hours of his arrest and thereafter not less than once every ten days.

(b) The magistrate shall at every appearance of such person before him enquire whether he has satisfactorily replied to all questions at his interrogation and whether it will serve any useful purpose to detain him further.

(c) Such person shall be entitled to be assisted at his appearance by his legal representative.

(5) Any person detained in terms of this section may at any time make representations in writing to the magistrate relating to his detention or release.

(6) No person, other than an official in the service of the State acting in the performance of his official duties-

(a) shall have access to a person detained in terms of this section, except with the consent of the magistrate and subject to such conditions as he may determine: Provided that the magistrate-

(i) shall refuse such permission only if he has reason to believe that access to a person so detained will hamper any investigation by the police;

(ii) shall not refuse such permission in respect of a legal representative who visits a person so detained with a view to assisting him as contemplated in subsection (4) (c); or

(b) shall be entitled to any official information relating to or obtained from such detainee.

(7)(a) Any person detained in terms of this section shall-

(i) as soon as possible be examined by a district surgeon; and

(ii) not less than once every five days be visited in private by a district surgeon,

and such a district surgeon shall as soon as possible compile a report in respect of each such visit and submit it to the magistrate.

(b) The magistrate may, if he has reason to believe that it will not hamper any investigation by the police, furnish at the request of any particular detainee a copy of any report referred to in paragraph (a) to a person indicated by that detainee.

(8) For the purposes of this section 'magistrate' includes an additional magistrate.

to submit at such time and place as may be determined by the police official, any such register, record or document. It further provides that the official may examine any such register, record or document or make an extract therefrom or a copy thereof, and require from any person an explanation of an entry in any such register, record or document. The only safeguards contained in the Drug and Drug Trafficking Act are that information must be submitted to the magistrate on oath by the Director of Public Prosecutions concerned, or by any public prosecutor authorized thereto in writing by that Director of Public Prosecutions, that there are reasonable grounds for believing that any person is withholding any information as to a drug offence, from that attorney-general, any public prosecutor or any police official, as the case may be, and then the magistrate may issue a warrant for the arrest and detention of the person concerned. The incentive for providing information under both Acts is to escape detention. It seems that the effect of a directive issued under the Interception and Monitoring Prohibition Act is more direct in the sense that the party holding certain information is ordered to present the information to the police official. The provision does not leave options to the person to withhold the information as long as possible and to give up the information shortly before the appearance before a judicial official, as the Criminal Procedure Act does. The need for the existence of different methods of enabling law enforcement agencies to obtain call-related information seems questionable. The Commission is therefore of the view that the Interception and Monitoring Prohibition Act should be the only Act to authorise the request for call-related information and should exclude the use of any power in any other Act, to obtain evidence or information in respect of a person, body or organization.

(b) Recommendation

12.2.20.6 Hence, the Commission recommends the insertion of clause 5B(4) in the Act making provision that the availability of the procedures set out in the Act in respect of the ongoing provisioning of call-related information excludes the use of any power in any other Act, to obtain evidence or information in respect of a person, body or organization.

12.2.21 Clause 5B(5): keeping proper records regarding identities and addresses

(a) Comments on the proposed clause

12.2.21.1 Telkom considers that the practicality of these requirements are questionable,

particularly with respect to where services are contracted telephonically. Telkom states that it is also not clear for what period these records are required to be kept. Telkom remarks that the provisions of clause 5B(7)(b) as is currently drafted, unfairly limits Telkom's contractual freedom to decide the basis on which to contract with its customers.

12.2.21.2 MTN considers that it is the intention of this sub-clause that a Network Operator shall ensure that proper records regarding identities and addresses are kept in respect of clients to whom telecommunications services are contracted whether on a prepaid or contract basis. MTN notes firstly that it is impossible for a Network Operator such as MTN to keep proper records regarding identities and addresses of such clients, due to the structure of appointing Service Providers to act as a distribution channel. MTN suggests that if it is the intention of the legislature to ensure and oblige MTN to keep track of addresses of Prepaid phone users then the legislature and Government will be capable of closing down a particular market addressed by MTN, and Vodacom for that matter. MTN notes that this would therefore mean that the Government would not only be interfering with the contractual obligations of MTN but also interfere with the commercial freedom of MTN. MTN remarks that in assessing the telecommunications market, they realised that many people in the Republic of South Africa, particularly in the informal sector, will not pass the credit vetting procedures established. MTN therefore implemented the Prepaid system and to allow for access by as many users as possible and created a distribution system through various retail and other outlets across the country. MNT considers that this, however, will come to naught if the current proposals are accepted. MTN suggests that as the proposed sub-clause 7 currently stands, MTN would be obliged not only to ensure that all details are taken and kept by such retail outlets but would oblige MTN to create such an additional administrative personnel to keep track of all of such records.

12.2.21.3 MTN considers that in ensuring that proper records regarding identities and addressee are kept, the question needs to be asked as to whether MTN or any similar company would therefore have to become experts on identity documentation or on addresses. MTN remarks that the current wording would suggest that MTN should know that an ID book is false or that an address given by a prospective client is non-existent or fictitious and that this surely cannot be the intention of the Legislature. MTN states that it cannot be emphasised enough, that should MTN or any similar Licensee be obliged to keep such detail of prepaid, such prepaid service as offered by MTN and similarly licensed Operators in South Africa will become

impossible. MTN notes that this would furthermore be in direct contradiction to the stated Government Policy of increased tele-density and accessible telecommunications for all in South Africa.

12.2.21.4 Vodacom remarks that regarding contracted subscribers, the directives should contain a request for identity information, which will be obtained by Vodacom from its service providers. Vodacom suggests that this information should, however, be that level and type of information obtained normally in the course of a commercial transaction of the instant type, and that it should not have to be information of the level required, for example, to register or transfer a motor vehicle. Vodacom states that as for requiring such information in respect of pre-paid users, the Commission (and the Government) need to give due regard to the objectives of the Telecommunications Act, 1996, in respect of achieving universal service through the development and distribution of affordable telecommunication services and products. Vodacom explains that the price and success of Vodago and other pre-paid products (these already constitute over 50% of Vodacom subscribers) are inextricably linked with ease and lower cost of distribution. Vodacom considers that to impose an identification procedure which, it appears, would have to be based on identity documents or company registration certificates, will result in the commercial decline, if not demise, of the product. Vodacom suggests that this would be counterproductive to the achievements of the objects of the Telecommunications Act. Vodacom remarks that one need only consider the cost of the national motor vehicle registration or gun licensing system to appreciate the potential cost implications of complying with such a requirement. Vodacom considers further that the Commission has not considered the problems associated with knowing the identity of an international roamer on a mobile network whose identity is unknown. Vodacom proposes the following clause:

> Any person, body or organisation rendering a telecommunication service shall,
>
> (a) ensure that proper records regarding addresses and identities are kept in respect of clients to whom a telecommunication services are contracted; provided that pre-paid users shall be excluded from this obligation;
> (b) require positive identification from a client to whom such a service is contracted, provided that pre-paid users shall be excluded from this obligation.

12.2.21.5 The Office of the Director Investigating Directorate Organised Crime and Public Safety and the Office of the Director of Public Prosecutions of the Cape of Good Hope remark as follows:

> Hierdie wysiging word deur Respondent ondersteun, rnaar daar word aanbeveel dat dit ook uitgebrei word na die verkoop, skenk, oorhandiging ens. van selfone deur "geregistreerde eienaars" aan ander persone asook die verkoop en handel van tweede-handse selfone. Respondent beveel aan dat daar 'n verpligting geplaas word op alle gebruikers van selfone om inligting ten opsigte van die fisiese gebruik van die selfone aan die diensverskaffers te verstrek. Dit sal byvoorbeeld sinneloos wees indien 'n selfoon gebruiker 'n vreemdeling kan gebruik of een van sy makkers gebrulk om die selfoon aan te koop en te kontrakteer terwyl die werklike gebruiker daarvan die sindikaatleier of sy meelopers is. Daar word voorgestel dat elke selfoongebruiker verantwoordelik gehou moet word vir elke persoon wat sy selfoon aanwend vir kommunikasie. Daar word voorgestel dat daar maandeliks by die betaling van die rekening inligting verskaf word deur die kontrakterende. party oor welke persone sy selfoon gebruik het buiten homself. In die gevalle waar die "pay as you go" betalingstelsel gebruik.word moet daar 'n verpligting op die selfoongebruiker geplaas word om maandeliks aan sy diensverskaffer inligting te verstrek oor wie almal sy selfoon benut het. Daar word, ook voorgestel dat daar 'n sanksie in gedagte gehou word vir die nie-nakoming van bogenoemde vereistes.

12.2.21.6 Ms Naicker[72] considers that it is reasonable to expect records to be kept of the contract based users. She points out that it is a requirement that they disclose full details namely name identity numbers and addresses when entering into a contract. She considers that the other issue that usually must be taken into account is that persons who use the prepaid service do so, so that no records are kept of them as with the contract-based users. Ms Naicker states that this will place an onus on retailers authorised to sell the prepaid vouchers to obtain this information from the users on a regular basis. She considers that this will be a very difficult task to monitor and control. She suggests that the idea of having lists of the various users is directly intrusive on the users and therefore this must be correctly implemented. Ms Naicker notes that persons who will provide incorrect information in order not to disclose their personal details will further impede the task. Ms Naicker considers that "positive identification" should be interpreted as a National identity document or a passport. She states that no other identification shall be acceptable and that no exceptions to this rule shall be accommodated.

12.2.21.7 SATRA considers that the proposed provision seeking to impose an obligation to keep records of clients to whom telecommunication services are provided is somewhat more problematic. SATRA notes that the right to publish or communicate anonymously could be regarded as being inherent within the right of freedom of speech. SATRA considers that the

---

72 Of the Department of Public Works.

identity of the communicator is surely no different from the other components of the document's content that the author is free to exclude or include. SATRA points out that parties may want to communicate with others of like-minded views, but may fear retribution for doing so and that they may therefore choose to act anonymously or with e-mail addresses that do not fully identify them. SATRA notes that this type of communication plainly implicates the constitutional protection for freedom of association.

12.2.21.8 SATRA considers that the provision that obliges telecommunication service providers to keep records of customers does also not take into account the phenomenon of so-called Internet cafes. SATRA notes that telecommunications customers apply, via a computer terminal and modem at the Internet cafe, to Internet Service Providers such as hotmail for an e-mail address. SATRA points out that the service is free and there is no need for the Internet Service Provider to be appraised of the customer's full details. SATRA states that the largest online networks routinely assign e-mail addresses to their customers using numbers and/or nicknames and that it is the very nature of the Internet to deliver information via e-mail addresses that are less than fully identifiable. SATRA notes in addition, that it is possible to 'surf the net' and 'chat' with other Internet users and that an e-mail address is not even required for this activity. SATRA considers that this chit-chat is certainly a form of telecommunication and it would be impossible to keep records of all customers who make use of this type of telecommunication service without infringing of fundamental freedoms entrenched in the Constitution such as freedom of speech, freedom of association and privacy.

(b) Evaluation

12.2.21.9 The project committee was of the view that it is appropriate that the persons, bodies or organisations rendering a telecommunication service should be obligated to obtain the prescribed information when they sell a phone to the customer who has contracted for the use of a telecommunication service. The committee took into account that any person may buy a phone and noted the objections raised against the imposition of the obligations set out in the clauses. The committee however considered that the telecommunication service providers should be under the obligation to obtain the required information from their customers otherwise all criminals will make use of the pay as you go system. The committee noted that, as was commented to the committee by the law enforcement agencies, if the Bill requires the ascertaining of identification, law enforcement will at least have the benefit of having a starting

point in their investigations when trying to establish who the culprits are that are involved in crime. The committee noted the objections some respondents raised on the drastic influence the clause will have on prepaid telephony. The committee was concerned about the issue whether the objections are not based merely on sheer commercial considerations. The committee considered that it is entirely appropriate to require positive identification from a client to whom telecommunication services are contracted and that identification is already required in any event when a client acquires a contract.

12.2.21.10 The committee also considered whether clause 5B(7)(b) should specifically set out that it applies also in respect of prepaid services but noted that the wording "to whom such a service is contracted" and concluded that it refers back to clause 5B(7)(a) and that prepaid and contracted services are therefore covered by the clause.

12.2.21.11 The Commission is also of the view that it is entirely appropriate to impose the obligation on telecommunication service providers to ensure that proper records regarding identities and addresses are kept in respect of clients to whom telecommunication services are contracted and to require positive identification from such clients.

(c) Recommendation

12.2.21.12 The Commission recommends that the Bill set out an obligation requiring telecommunication service providers to ensure that proper records regarding identities and addresses are kept in respect their clients to whom telecommunication services are contracted and to require positive identification from such clients.

12.2.22 Clause 5B(6): provision of information regarding identity[73]

(a) Comments on the proposed clause

12.2.22.1 Telkom states that aside from defining, by reference to section 3(2), which persons are entitled to request the information, this subsection does not make the request subject to a directive by a judge in terms of the Act. Telkom points out that any of the said

---

73 Clause 5B(5) in the discussion paper.

persons can therefore request the information at any time in order to "fulfil the functions and exercise the powers authorised by law" but not necessarily by this Act. Telkom considers that it would then have no means of ascertaining whether a person requesting information is entitled to make the request or if the request is in fact legal.

12.2.22.2 Telkom suggests that the word 'users" should generally be replaced with the word 'customers" and suggest that the words "the person using' should be replaced with the words 'the customer who has contracted for the use of'. Telkom points out that no telecommunication service provider can provide information on the identity of the user of a telecommunication system. Telkom suggests that this is irrespective of whether the user uses a public telephone such as a payphone or whether the user uses a telephone for which someone has entered into a contract with the telecommunication service provider. Telkom remarks that the telecommunication service provider can only supply information in respect of the party who has contracted for the service. Telkom notes that where a legal entity other than a natural person has contracted with the telecommunication service provider, the provision of the required information becomes even more problematic. Telkom points out that the telecommunication service provider has no access to the required information for the users of PABX extensions, users of prepaid cards, coin-phones, card-phones and the customers of other networks accessing customers of its network.

12.2.22.3 Telkom suggests that clauses 5B(6) and 5B(7)[74] be deleted in its entirety as it is in conflict with the Act.

12.2.22.4 Vodacom proposes the deletion of clause 5B(6) stating that it does not support the inclusion in the act of a separate enabling clause for obtaining information outside the context of a directive.

12.2.22.5 MTN notes that the word "users" appears in this particular clause. MTN believes that "users" should be defined as being the owner of a telecommunications device, as "users" indicates that all people that utilise a particular telecommunications service falls within the ambit of this particular clause. MTN points out that a "user" could be totally anonymous to a Network Provider as only the Owner of that particular telephone or telecommunications service is

---

74 Clauses 5B(5) and (6) of the Bill in Annexure C, which was contained in the discussion paper.

recorded. MTN considers that should a person, other than the owner utilise such telecommunications services, it is impossible for the Network Operator firstly to know this and secondly to provide information such as the name, identity number and address of "the user" of a specific telecommunications number.

(b) Evaluation

12.2.22.6 The project committee noted that in terms of the proposed clause an officer or member does not need to apply to a judge to authorise the provision of the information to him or her. The committee was satisfied that the officer may obtain such information without obtaining a directive first. The committee noted that in the normal course of police work, for example, the officer may request information without necessarily having to obtain a warrant. The committee noted that the provision concerns the retrieval of information. The committee was satisfied with the principle contained in the provision, assuming that the correct information is at issue and it is a qualified person who may request that the information be provided without him obtaining a directive first. The committee noted that this clause does not deal with monitoring and that the officer or member concerned may probably be merely following up on information which he or she already has. The officer might have monitored a target, obtained information and then wishes to ascertain for example who bought the telephone, whether there was a change of address etc. The committee considered that the obligation imposed on the telecommunication service providers is indeed one that should be possible under the Act.

12.2.22.7 The Commission is also of the view that the proposed obligation imposed by the clause should be one that should be possible under the Act and in the terms as worded in the proposed provision. The Commission has also noted the comment made by Telkom which suggests that the word 'users" should generally be replaced with the word customers" and that the words "the person using" should be replaced with the words "the customer who has contracted for the use of". The Commission considers Telkom's reasoning that no telecommunication service provider can provide information on the identity of the user of a telecommunication system persuasive.

(c) Recommendation

12.2.22.8 The Commission recommends that the provision as proposed in the discussion

paper be included in the Bill but that the term "user" and "the person using" be replaced as Telkom suggested namely:

> Any person, body or organization rendering a telecommunication service, shall provide such information regarding customers of such telecommunication service to the South African Police Service, the South African National Defence Force, the Agency or the Service, as may be required by an officer or member referred to in section 3(2)(a), (b) and (c) to fulfil the functions and exercise the powers authorized by law.

12.2.23 Clause 5B(7): provision of name, identity number and address of person contracted for the use of a specific telecommunications number

(a) Comments on the proposed clause

12.2.23.1 The National Intelligence Agency[75] considers that the words "and, where applicable, the equipment number" should be inserted in section 5B(7). They remark that it is foreseeable that differences in interpretation will arise between the network and service providers on the one hand, and government agencies on the other. The NIA suggests that it could therefore be considered to provide for a speedy dispute resolution mechanism that could involve the Minister responsible for Posts, Telecommunications and Broadcasting, or someone designated by him or her. The NIA points out that this should, however, not exclude possible court action by the dissatisfied party if the latter wants to do so. Vodacom suggests the following clause:

> The obligations in terms of subsection(5) includes the provision of the name, identity number and address of a contracted client referred to in section 5B(5), using a specific telecommunications number.

(b) Evaluation

12.2.23.2 We noted above that the project committee and the Commission are of the view that obligation imposed on the telecommunication service providers to provide certain information to the Police, the Defence Force, the National Intelligence Agency and the Secret Service is indeed one that should be possible under the Act. Clause 5B(7) provides merely further particulars on the information that may be requested. The project committee and the

---

75 Deputy Director-general Operational Services.

Commission are of the view that this provision is appropriate and that the clause as contained in the discussion paper should be included in the Bill except for the replacement of the phrase "the person using" with the words "the customer who has contracted for the use of".

(c) Recommendation

12.2.23.3 The Commission recommends that clause 5B(7) prescribe that the obligation in terms of subsection (5) includes the provision of the name, identity number and address of the person contracted for the use of a specific telecommunications number.

12.2.24 Clause 6: urgent applications

(a) Comments on the proposed clause

12.2.24.1 Ms Naicker[76] notes that it is important that the Act makes provision for urgent applications where the judge may dispense with set procedures. She considers that the judge should be given the authority to make an oral direction followed up by a written direction within 1 week. She considers that the approach followed by the Americans is reasonable and that if an application is made as one of urgency and the usual procedures have not been followed, the applicant must ensure that a proper application is made within 48 hours of the interception or monitoring. She notes that this will create transparency in the law. Ms Naicker suggests that due to the urgency of the application the interception must cease once the necessary information has been obtained or if on a proper application the judge has subsequently denied that application. She considers that this clause shall place a duty on the applicant to show that the application was indeed urgent. She suggests that apart from the judicial discretion that will be applied the applicant must meet the following requirements:

(a) that the information that has to be intercepted cannot be obtained at any other time and if the interception does not occur it shall amount to a miscarriage of justice,
(b) that the activities to be monitored are of such nature that they threaten the national security of the Republic, or
(c) that there exists immediate danger of death or serious physical injury to any person.

---

76 Of the Department of Public Works.

12.2.24.2 Ms Naicker proposes that the proposed interception or monitoring based on an urgent application shall extend for the duration of only 2 weeks or until the relevant information is obtained at which stage the interception and monitoring should cease.

12.2.24.3 Telkom considers that there is no way that a telecommunication service/network provider will know that an oral direction has been given by a judge, unless such direction is also made directly to a telecommunication service/network provider. Telkom suggests that the Act should accordingly be amended to indicate that when the judge makes an oral direction, the judge should make the same direction orally to the telecommunication service provider's representative. Telkom proposes the following amendment:

> The judge referred to in subsection 3(1)(a) may in any case considered by him or her to be sufficiently urgent, dispense with the procedure contemplated in subsections (1) and may deal with the matter in such manner and subject to such conditions as he or she may deem fit, including the grant in any appropriate case of an oral direction in which instance such oral direction shall also be made to the representative of the telecommunications service provider followed up by a written application within one week".

12.2.24.4 MTN agrees that a panel of judges be appointed as suggested. MTN is concerned that oral directives may be granted. MTN considers that this is problematic in that such oral directive shall only be "followed up by a written application within one week" and it does not contemplate the issue of a written directive thereafter. MTN is of the view that to be able to protect its customers as well to avoid any mistakes only written applications and directives be allowed. MTN considers that another interpretation of the particular clause could be that the security structure applying for the directive, could, after having been granted such directive on an oral basis, also on an oral basis approach the Network Operator to do the necessary monitoring. MTN notes that clearly this cannot be the intention of the Legislature and therefore it is suggested that the Clause be deleted in its entirety or suitably amended.

12.2.24.5 The Law Society of SA's standing committee on constitutional affairs considers that the Bill should set out more detailed procedures to be followed in the case of urgent applications. The Law Society's Committee considers that simply allowing the judge to dispense with the procedures set out under section 6(1) and to "deal with the matter in such manner and subject to such conditions as he or she may deem fit" may lead to abuse. The

Committee suggests that procedures in the case of urgent applications could, on the Hong Kong and Canadian models, place a time-limit within which an application for a proper directive must be lodged. The Committee considers that the Bill should also describe exactly under which circumstances a case would be "sufficiently urgent" as to allow a judge to dispense with the procedures under section 6(1).

12.2.24.6 The Office of the Director Investigating Directorate Organised Crime and Public Safety and the Office of the Director Public Prosecutions Cape of Good Hope remark as follows:

> In beginsel ondersteun Respondent die invoeging van 'n dringende aansoek prosedure. Die mondelingse aansoeke en magtiging word egter nie deur Respondent ondersteun nie. Die rede hiervoor is dat daar legio bewysregtelike probleme in die verband kan ontstaan. Dit het reeds in die verlede gebeur dat regters mondelings magtiging gee wat dan later opgevolg word met die skriftelike magtiging. Wat in die praktyk egter kan gebeur, is dat 'n regter byvoorbeeld sodanige magtiging kan verleen maar weens 'n siektetoestand nie beskikbaar is om 'n geskrewe magtiging te verskaf nie. Daar is ook die moontlike probleem dat dit wat aan die regter rnondelings meegedeel word kan verskil van wat later in die voorgestelde week periode skriftelik aan hom voorgelê word. Dit is Respondent se voorstel dat daar rekord gehou moet word en veral volledige rekord ten opsigte van 'n rnondelingse aansoek en magtiging. In die verband beveel Respondent aan dat van sodanige aansoek en magtiging rekord gehou kan word deur die gebruikmaking van audiobande.
>
> Daar moet ook in gedagte gehou word wat die effek sal wees indien daar 'n mondelingse aansoek was en 'n mondelingse magtiging deur die betrokke regter verleen is, maar dat dit nie opgevolg word deur 'n skriftelike magtiging soos deur die wet vereis is nie, weens onvoorsiene omstandighede. Die vraag wat nou ontstaan is, sal hierdie aansoek en magtiging nietig wees of sal dit slegs vernietigbaar wees?
>
> Respondent is 'n groot voorstaander van 'n dringende aansoek prosedure maar wil voorstel dat hierdie dringende aansoek prosedure uitdruklik en volledig in die wet omskryf word en wil aanbeveel dat die riglyne van die Verenigde State van Amerilca en Kanada gewensde riglyne is om na te volg.

12.2.24.7 Adv JT Molefe remarks that there is always a judge in South Africa available to deal with these in the context of general legal applications and there is no reason to deal with urgent interception/monitoring applications elsewhere than in court, irrespective of date, time or day of the week. He remarks that in short, executive action that intrudes on people's basic human rights and economic freedom, cannot be justified on the grounds of urgency. He considers that Rules of court are present to deal with general urgent applications and these can also be made to apply to interception/monitoring applications. He is however of the view that

urgency as where an interception to prevent bodily harm is sought might justify radical departure from the rules and accommodate methods such as, for example; a telephonic application to a judge.

12.2.24.8 The SAPS[77] remarks that the proposals relating to emergency applications are strongly supported. They note that in practice, the South African Police Service has experienced a number of instances where such a procedure would have been useful, eg. cases of hostage-taking. The SAPS suggests that although action could have been taken in terms of the common law principles of emergency, it is preferred that the proposed procedure be created in the Act.

12.2.24.9 Vodacom states that it accepts that provision should be made for procedures in respect of urgent applications. Vodacom points out that it is not clear what the Commissions means by the words "oral directive" in respect of the proposed insertion to section 6 of the draft Bill, and therefore it is proposed that it be formulated in clearer language. Vodacom proposes that the judge be entitled to dispense with the written application procedure, but that the directive still be in writing in order to protect both the individual being monitored and the network operator. Vodacom considers that in such cases, a judicial indication of the directive's relative priority to all other existing directives issued to the network is critical. Vodacom submits that the duration of this type of urgent directive be limited to 48 hours, without further renewal on an urgent basis, and by then, a normal application must have been made, and a normal directive obtained. Vodacom suggests in its subsequent submission that although the judge should be entitled to dispense with the written application requirement, the directive should still be in writing in order to protect both the individual being monitored and the network operator. Vodacom proposes the following clause:

> The judge referred to in subsection 3(1)(a) may in any case if considered by him or her to be sufficiently urgent, dispense with the procedure contemplated in subsection (1) and may deal with the matter in such manner and subject to such conditions as he or she may deem fit, including the grant in any appropriate case of a direction on an oral application, provided that a written application will be submitted within one week.

12.2.24.10 Judge Gordon states that he agrees with the amendment which he considers important to include. He states that he is pleased to see it is his draft which he did after a

---

77 Chief Manager Legal Component Detective Services.

series of detailed discussions. He considers it adequate to deal with the important question of urgency.

12.2.24.11 The NICOC subcommittee suggests that any direction given by a judge in an urgent matter should always be in written form. They however consider that the judge should be in a position to consider an oral application, followed by a written one.

(b) Evaluation

12.2.24.12 The committee noted that the clause makes provision for the issue of an oral directive and that a written application must be furnished to the judge concerned within one week. The committee considered whether the Bill ought not to require a written directive in all cases. The committee considered that there might be cases where a written application is not furnished to the judge within one week. The committee suggested that something might happen and the whole case falls through, and as a result of the oral directive issued and what was done in terms thereof, claims are instituted and litigation ensues. The committee considered whether there should not be a mechanism for recording the oral directive and to prevent the misinterpretation of an oral directive. The committee noted that ideally the applicant produces a written application within a week and a written directive is then issued.

12.2.24.13 The committee noted that the proposed clause envisages an oral directive, followed up by a written application and it considered whether it should not be required that the oral directive should also be reduced to writing. The committee considered the setting out in the Bill of the power of the Minister of Justice to issue regulations prescribing everything done under the Act, including the keeping of records of applications made in writing or orally in terms of the clause. Ordinarily, in other cases there would be a record in the Registrar's office but by the very nature of these applications such a record could not be kept in the office of the registrar. The project committee was therefore concerned that clause 6(2) could be meaningless. The committee noted that if there is not some sort of prescribed system of record keeping, there may be opportunity for the process being abused. The committee therefore resolved that the words "incorporating the terms of the oral directive" should be inserted in clause 6(2), after "followed up by a written application, within one week". The committee also resolves that a proviso be added to subclause 6(2), namely "Provided that in all cases where an oral directive was issued, such directive shall be reduced to writing within two days".

12.2.24.14 The Commission shares the concern of the project committee that the Bill should prescribe that oral directives should be reduced to writing. The Commission is of the view that the wording suggested by the project committee is appropriate.

(c) Recommendation

12.2.24.15 The Commission recommends that the Bill makes provision for the judge being able to dispense with the procedure set out in the Act for applying for a directive in circumstances which he or she considers to be sufficiently urgent. The Commission recommends that the proposed clause prescribe that an oral directive may be granted by the judge which is followed-up within a week by a written application incorporating the terms of the directive and, furthermore, that where an oral directive was issued, the judge's oral directive must be reduced to writing within two days.

12.2.25 Clause 6A(1): evidence is subject to the decision of a Director of Public Prosecutions or an Investigating Director

(a) Comments on the proposed clause

12.2.25.1 The SAPS[78] notes that the comments from the corps of the directors for prosecution will be important in this regard. The South African Police Service would accept the opinion of the National Director of Public Prosecutions in this regard. The SAPS considers that in view of the fact that monitoring may be done only in respect of "serious crime", it might ensure that the evidence so obtained will be used responsibly.

12.2.25.2 Ms H Naicker[79] considers that it is important that the material obtained from monitoring can only be used as evidence with the authorisation of the Director of Public Prosecutions or Investigating Director or any person authorised by them. She remarks that this creates a check and balance with regard to whom shall have access to the information. She points out that if this provision is not well monitored the credibility of the criminal investigative unit will be placed in question as there would be risk of the information or evidence being

---

78 Chief Manager Legal Component Detective Services.

79 Of the Department of Public Works.

disclosed to various parties.

12.2.25.3 Judge Gordon notes that the question of using information obtained through the application of the Act in Court, is a point repeatedly raised by him in the light of certain criminal trials where, unbeknown to him, such evidence was used. He says he suggested that no such evidence be led without special authorization from the provincial Attorney-General. He points out that the obvious reason was to protect other sensitive evidence from being made available (selective evidence would not be allowed) and also, to prosecute on this evidence alone (without corroboration of direct evidence) would usually be inadvisable and undesirable. He notes that he invited the Deputy Attorney-General of the TPD to attend such discussion and that his views were positive. In the circumstances Judge Gordon remarks that he is pleased to agree to this amendment.

(b) Evaluation

12.2.25.4 The project committee noted the prosed clause and considered whether the clause does not raise the issue of the separation of powers since the clause is vesting in the Directors of Public Prosecutions the power to exclude relevant evidence from a court. The committee noted that if the concern was the potentially deleterious effect of presenting such evidence in court where the police might still be following up on the evidence, then the prosecution runs the risk if they proceed to trial and they for reasons flowing from whatever directive of the Director, wish or do not wish to lead the evidence in court. The committee therefore considered that the provision is appropriate and should defence counsel wish to obtain such evidence, the defence may serve a mandamus on the Director. The evidence might be exculpatory and might be vital to establish the accused's defence. The committee however considered that the prosecution has such power in any case and provided there is no legitimate claim to confidentiality, the defence would be entitled to such evidence.

12.2.25.5 The project committee also considered whether there is a need for clause 6A: the committee noted that the Director of Public Prosecutions has anyhow the power set out in clause 6A(1) and a court can decide whether the evidence is admissible which clause 6A(2) seeks to govern. The committee however noted that the proposed clause seeks to lay down a basis in law to regulate these aspects. The committee resolved to retain the two subclauses but to state that it is doubtful whether these clauses add anything at all.

12.2.25.6 The Commission is of the view that the project committee identified the issue correctly when arguing that the aim of the provisions concerned is to lay down a basis in law to regulate these aspects. The Commission considers, furthermore, that although the Directors of Public Prosecutions may already have the power to lay down guidelines on which evidence may or should be presented to court, as the project committee pointed out, it is appropriate to set these powers out in the Interception and Monitoring Prohibition Act. The Commission is therefore in favour of the inclusion of the clause.

(c) Recommendation

12.2.25.7 The Commission proposes that the amendment Bill provide that the use of any information obtained through the application of the Act, or any similar Act in another country, as evidence in any prosecution, is subject to the decision of the Director of Public Prosecutions or an Investigating Director contemplated in the National Prosecuting Authority Act, 1998 (Act No 32 of 1998) concerned.

12.2.26 Clause 6A(2): admissibility of evidence obtained as a result of monitoring/interception

(a) Comments on the proposed clause

12.2.26.1 The Law Society of SA's Standing Committee on Constitutional Affairs states that only information obtained on the grounds on which the directive was originally granted, should be admissible. They note that, as was pointed out in the discussion document (par 9.17) "fishing-expeditions" or exploratory interceptions" are not allowed under the German system. The Committee points out that a judge would only issue a directive if he or she is convinced that the grounds enumerated in clause 3 (b) are present. The Committee states that allowing evidence obtained in terms of a lawful direction, but in respect to an offence other than the one for which direction has been granted, could open a back-door for exploratory interceptions. They consider that an applicant who is unable to satisfy the requirements in clause 3(b) to obtain a directive, could now under the cover of a different directive obtain such evidence. The Committee states that the Act (section 2(1)) and the discussion document (p ix) confirms the basic principle that the interception and monitoring of conversations and communications is prohibited. The Committee notes that the Act sets stringent requirements on the acquiring of

directives to intercept and monitor conversations and communications. The Committee considers that it should be carefully avoided to create a loop-hole in the Act in terms of which these stringent controls can be circumvented.

12.2.26.2 The Law Society's Committee points out that the Act provides a valuable tool in the combatting of serious offences. They consider however, that because the monitoring and interception of communications constitutes a serious inroad into the right to privacy and bearing in mind that the Constitution provides that evidence obtained in a manner which would violate any right in the Bill must be excluded (section 35(5)), the Act must be as clear and detailed as possible in setting out the procedures to be followed. They consider that detailed procedures, especially in the case of urgent applications, would also prevent abuse of the powers granted in terms of the Act.

12.2.26.3 The SAPS[80] remarks that interception and monitoring may be authorized in respect of serious offences which have been committed, which are in the process of being committed, and which will probably be committed. The SAPS points out that as an investigation method, it may be used also to prevent crime - if the South African Police Service executes a direction for monitoring in respect of drug trafficking and evidence of a murder emanates from such execution, the South African Police Service will be duty bound to investigate the murder. (The evidence or information derived in this manner could not have been obtained unlawful, because the South African Police Service have obtained a direction to monitor the said conversations). The SAPS states that furthermore, the success in combatting organized crime lies in a holistic approach - the structure of crime syndicates has to be dismantled by acting in every possible legal way - civil and criminal forfeiture, prosecution for any possible offence, including tax evasion, etc.

12.2.26.4 The SAPS notes that there are examples in legislation of other countries where the principle is accepted that such evidence obtained from a lawful interception may be used in a prosecution unrelated to the direction. (They point out the Netherlands legislation referred to in the Discussion Paper). They consider that a case can be made out that such a provision will not be unconstitutional.

---

80 Chief Manager Legal Component Detective Services.

12.2.26.5 The Office of the Director Investigating Directorate Organised Crime and Public Safety and the Office of the Director Public Prosecutions Cape of Good Hope remark as follows:

> Die Respondent ondersteun hierdie beoogde wysigings, maar wil aanbeveel dat die beoogde wysiging wat lees 'irrespective of the grounds on which or the offence in respect of which the alteration was obtained', die gewensde bepaling is. Ondervinding het geleer dat veral by georganiseerde misdaad en veral georganiseerde misdaad waar daar dwelmhandel by betrokke is, daar ook verskeie ander misdrywe tydens die monitering van die betrokke individue se telefone opgetel word. So het dit dan al ook in die praktyk gebeur dat daar magtiging ontvang is om 'n spesifieke individu se telefoon te monitor vir dwelmhandel ondersoekdoeleindes en dat die verdagte onderwerp betrokke was in 'n opspraakwekkende moord. Dit sal tragies wees indien daardie inligting nie in 'n kriminele hof aangewend kan word as getuienis nie omdat die magtiging om mee te luister bekom is vir dwelmdoeleindes en nie vir die pleging van die moord nie, en slegs om daardie rede uitgesluit word.
>
> Respondent wil dus aanbeveel dat die bepaling ten minste die volgende moet duidelik stel:
>
> a) Dat alle inligting bekom, aangewend kan word teen enige party hetsy hy 'n party tot die gesprek was of nie;
>
> b) Dat alle inligting aangewend kan word in enige klag ongeag vir watter doel die magtiging bekom is.
>
> Hierdie inligting moet selfs toelaatbaar wees ten opsigte van die misdaad waarvoor daar nie magtiging bekom is nie en al is alle "less intrusive' ondersoekmetodes nie uitgeput nie.

12.2.26.6 The Cape Law Society's Law and Procedure Committee proposes that the provisions contained in the Hong Kong Interception of Communications Ordinance on the admissibility of evidence should be included in our legislation.

12.2.26.7 Ms H Naicker[81] considers that any evidence that is obtained in a procedurally correct manner and that is of relevance to the case at hand shall be admissible. She says that the further discretion remains with the judge when analysing the evidence that is presented. She suggests that the onus will then rest on the defence to challenge the admissibility, legality and relevance of the evidence. She notes that the next issue that arises is information that is obtained where the direction did not cover the interception of such information. She points out that the defendant would ordinarily challenge this on the grounds that it would have been

---

81 Of the Department of Public Works.

illegally obtained. Ms Naicker suggests that the Commission must weigh up the interests of the individual against that of the criminal investigative process.

12.2.26.8 Ms Naicker remarks that if this situation arises which in all likelihood it shall, the Act should make provision for the fact that such evidence shall be deemed admissible where the investigative team makes use of this evidence within 1 (one) year of obtaining the information. She notes that this means that charges must be laid against the implicated individual by the Attorney General within one year of the interception of that non-directive information. She suggests that it must be shown further that the information would not have been ordinarily obtainable if the investigative team had to make a further application to monitor that individual. She considers that this system would assist the criminal investigative process in that perpetrators of serious offences shall not easily be able to thwart the process on the basis of a technicality.

12.2.26.9 MTN is of the opinion that alternative Clause 6(A)(2) would be more appropriate in the circumstances.

12.2.26.10 Vodacom considers that the relative ease and technological capacity to obtain information in this manner necessitates that State agencies should continue to bear the onus of proof as set forth in section 3(1)(b) of the Act. Vodacom remarks that taking into account that the primary purpose of the Act is to assist in the investigation of offences which would normally result in criminal proceedings, it is understandable that the onus of proof will not be "beyond a reasonable doubt" during the investigation phase. Vodacom however suggests that, taking into account the seriousness and potential extent of the intrusion into an individual's privacy, the normal law of evidence in respect of civil proceedings should apply and that the onus of proof should be specified in the Act to be "on a balance of probabilities".

12.2.26.11 The NICOC subcommittee considers that to combat organised crime, it is essential to be able to use all evidence, which is not privileged , irrespective of the crime for which the direction has been issued.

(b) Evaluation

12.2.26.12 The project committee considered which of the two proposed clauses on the

admissibility of evidence obtained under the Act is preferable. The committee took into account that an application may be made for an directive to be issued in regard of offence A and offence B is discovered as a result of the directive. The committee noted that there is strong support from the law enforcement agencies for the inclusion of these provisions into the Bill. The committee noted that under these circumstances the evidence is surely not tainted where law enforcement agencies stumble upon the serious offence under these circumstances. The committee took note of a case where for example an application is made for a directive on the suspicion of the target having committed money-laundering, the accused's door is broken down and it is established that he committed treason.

12.2.26.13 The committee also considered whether there is a need for clause 6A: the committee noted that the DPP has anyhow the power set out in clause 6A(1) and a court can decide whether the evidence which clause 6A(2) seeks to govern, is admissible. The committee however noted that the proposed clause seeks to lay down a basis in law to regulate these aspects. The committee resolved to retain the two subclauses but to state that it is doubtful whether these clauses add anything at all. The committee decided furthermore that the alternative clause 6A(2) is preferable since the proposed wording of clause 6A(2), namely "irrespective of the grounds on which the directive has been granted", may attract all sorts of arguments.

12.2.26.14 The Commission is of the view that although it might be correct to assert that the clause does not add anything new, legal certainty could be effected if the Bill were to set out what the consequences are if evidence is obtained as a result of a directive requested regarding the commission of a certain criminal offence, and information is obtained regarding the commission of any other serious offence. The Commission is of the view that such information should be admissible as evidence in criminal proceedings.

(c) Recommendation

12.2.26.15 The Commission recommends that information regarding the commission of any criminal offence obtained by means of any interception or monitoring in terms of the Act, or any similar Act in another country, may be admissible as evidence in criminal proceedings.

12.2.27 Clause 8: penalties

(a) Comments on the proposed clause

12.2.27.1 Ms H Naicker[82] notes that the penalties that are stipulated are reasonable, as non-compliance is a serious offence. She considers however, if the Network provider is given an initial subsidy to erect the interception equipment then the failure to maintain the equipment should carry a harsher penalty. She suggests that the failure to comply with the directive from the Minister should not lead to a possibility of revocation of the Network Providers licence but initially a suspension would be a reasonable alternative. She considers that if the Network Provider then fails to comply with any further directives, the revocation of the licence should be the final resort. She notes that in the circumstances R 200 000,00 as a maximum fine is appropriate taking into account that failure to maintain the network will impede the investigative process and render sections of the Act difficult to implement. She states that a duty rests on the Network Provider to maintain the network in order to give full effect to the Act.

12.2.27.2 MTN is of the view that it is wholly inappropriate to make a criminal of MTN for not complying with a directive issued by the Minister of Communications. The effect of the proposal is that MTN who renders a service, and if the intent of the Act is to be believed, without any cost to the State, is held to be in contravention of the Act and could loose its Licence.

12.2.27.3 Vodacom suggests that it is remarkable that the penalty for a violation of a "prohibition" Act's provisions in respect of unlawful monitoring and interception (see section 8(1)) is limited to R20 000-00 penalty and two years imprisonment, while failure to comply with a directive to install necessary equipment, to provide the necessary facilities or to comply with a judicial directive, carries a R200 000-00 penalty and the potential loss of one's licence. Vodacom submits that, assuming the current provision regarding the payment of a "reasonable remuneration" is retained, the proposed penalties will very likely prove to be unnecessary. Vodacom suggests that a more reasonable penalty be included in the Act.

12.2.27.4 Telkom considers that the obligations as currently set out in the Bill, are absolute and could be extremely onerous, and there is, therefore, a high risk that telecommunication service/network providers will be unable to comply.

---

82 Of the department of Public Works.

12.2.27.5 Professor Mervyn Dendy[83] states that two suggested amendments, one of which makes provision for a fine not exceeding R20 000 or imprisonment not exceeding two years for a certain offence, and the second of which makes provision for a fine not exceeding R40 000 or imprisonment not exceeding five years for another offence. He notes that the suggested maximum fines in these two provisions appear to have overlooked the provisions of the Adjustment of Fines Act 101 of 1991, section 1(2) of which deals with the question of maximum fines where a stated maximum period of imprisonment may be imposed in the alternative. He points out that in accordance with that provision, read with section 1(1)(A) of the Adjustment of Fines Act and section 92(1) of the Magistrates' Courts Act 32 of 1944, the maximum fine which a court may impose in lieu of a maximum period of imprisonment of two years is R40 000, and the maximum fine which may be imposed in lieu of five years' imprisonment is R100 000. He explains that this will override the suggested provision for maximum fines of R20 000 and R40 000 respectively in the two suggested amendments to the Interception and Monitoring Prohibition Act.

12.2.27.6 Prof Dendy remarks that he would accordingly suggest that no maximum fine be stipulated in either of the two proposed amendments, but that the amendments provide simply that the offender shall be liable on conviction to a fine or to imprisonment not exceeding the applicable period. He points out that on an application of section 1(1)(a) of the Adjustment of Fines Act, that will have the effect of allowing the court to impose maximum fines of R40 000 and R100 000 respectively for the two offences mentioned in the suggested amendments to the Interception and Monitoring Prohibition Act.

12.2.27.7 The SAPS[84] remarks that the fines proposed by the project committee, are strongly supported.

(b) Evaluation

12.2.27.8 The project committee noted the comments made by Prof Mervyn Dendy on the proposed clause and that the Adjustment of Fines Act, 101 of 1991 must have been overlooked and that he proposes that no maximum fine should be provided. The committee resolved that

---

83 Associate Professor of Law, University of the Witwatersrand.

84 Chief Manager Legal Component Detective Services.

his suggestion be adopted and that the phrases "not exceeding R 20 000" and "not exceeding R 40 000" in section 8(1)(a) and (b) respectively, be deleted.

12.2.27.9 The Commission is also of the view that Prof Dendy's suggestion is persuasive and that the Bill should be amended by the deletion in the proposed clauses 8(1)(a) and (b) of the set fines. The Commission has noted the objection in respect of the proposed maximum fines in regard to the offences proposed in clause 8(1A) but is of the view that the maximum amount of R 200 000 is appropriate taking into account the severity of the offences, particularly in view of the fact that the maximum fine which can presently be imposed in regard to a failure to desist from disclosing information is the amount of R 100 000. The Commission considers that a maximum fine for a failure by a telecommunication service provider to comply with a directive by a judge or the Minister of Posts, Telecommunications and Broadcasting to provide information regarding a customer contracted for the use of such service, to keep records or to require positive identification when contracting a telecommunication service is not excessive or inappropriate.

(c) Recommendation

12.2.27.10 The Commission proposes the deletion in clauses 8(1)(a) and (b) of the proposed maximum fines. The Commission however recommends in regard to clause 8(1A) that the maximum fine should be R 200 000 for the failure by a telecommunication service provider to comply with a directive, to provide information regarding a customer contracted for the use of such service, to keep records or to require positive identification when contracting a telecommunication service.

12.2.28 Clause 8A: revocation of licence

(a) Comments to the proposed clause

12.2.28.1 Telkom considers that in light of the lack of consultation in formulating the obligations imposed on telecommunication providers, this measure seems rather draconian.

12.2.28.2 In MTN's view this should be seen as an amendment to the current MTN Licence without complying with any of the provisions contained in the current Licence or the

Telecommunications Act and it is therefore our opinion that this particular Section should be deleted in its entirety.

(b) Evaluation

12.2.28.3 The project committee noted the argument of MTN who states that the provision should be seen as an amendment of MTN's current licence conditions without complying with any of the provisions contained in the current licence or the Telecommunications Act and that the provision should be deleted. The committee remarked that it does not follow the argument and does not support the suggestion.

12.2.28.4 The Commission is of the view that the proposed provision is appropriate and should be included in the Bill.

(c) Recommendation

12.2.28.5 The Commission recommends that the Bill should provide that if any person, body or organization rendering a telecommunication service, fails, after a conviction for failing to comply with a directive issued in terms of section 5A(6), to comply with a further such directive the Minister for Posts, Telecommunications and Broadcasting may revoke the licence issued in terms of Chapter V of the Telecommunications Act, 1996, to such person, body or organization to render a telecommunication service.

12.2.29 Regulating the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices

(a) Comments on the proposed clause

12.2.29.1 The Office of the Director Investigating Directorate Organised Crime and Public Safety and the Office of the Director of Public Prosecutions Cape of Good Hope remark as follows:

> Respondent beveel aan dat die besit, verspreiding, advertering van onderskep en meeluistering meganismes nie verbied word nie, aangesien dit net 'n verdere las sal plaas op 'n polisiemag wat reeds sukkel om uitvoering te gee aan bestaande

wetgewing, Indien persone hulle skuldig maak aan onwettige meeluistering of inbreuk maak op persone se privaatheid, pleeg hulle in elk geval 'n misdryf soos die wet tans lees en kan hulle in die verband aangespreek word. Dit is Respondent se respekvolle mening dat dit onnodig is om 'n verdere misdryf of verbod daar te stel. Die blote besit van meeluistering, opname en of ander apparaat is in elk geval skadeloos en dit is die onregmatige aanwending daarvan wat eintlik aangespreek moet word.

12.2.29.2 Ms H Naicker[85] considers that it is important that distinct sections be included in the Act in order to prevent the abuse of the system by so called "private investigators". She points out that it is important to note that a substantial number of these private investigators were members of various State organs. She states that the knowledge obtained while in the employ of the State is used to assist them in their private business. She notes that the monitoring of third parties by any person who is not a member of or authorised by the SANDF, SAPS, NIA and SASS should be an offence. Ms Naicker points out that it is important to note that the ordinary citizen whose privacy is invaded by a person who is not a member of the State in their official capacity shall have limited or no recourse to give effect to their rights in terms of the Constitution. She notes that the Constitution is of vertical application and the aggrieved person would usually have recourse where the State has infringed upon their rights and that where the infringement has taken place on a horizontal level the aggrieved party has to make an application to show the applicability of that section first. Ms Naicker considers that the cost involved in taking matter to the Constitutional Court is exorbitant; therefore the ordinary citizen would not effectively be able to be protected against ordinary persons violating their privacy.

12.2.29.3 Ms Naicker considers that this is the role that the legislation can play by protecting the ordinary citizen from the invasion into their privacy and she suggests that the stance that should be taken is as follows :

- the manufacture, distribution, possession and advertising of wire or oral communicating intercepting devices should be prohibited, unless-
- the person manufacturing, distributing, or who possesses the devices mentioned in (i) holds a licence issued by the Minister of Post and Telecommunication.

12.2.29.4 Ms Naicker remarks that if the above requirements are not met, the person in contravention of the law should be guilty of a statutory offence and shall be subject to a

---

85 Department of Public Works.

minimum fine of Rl 0 000,00 and maximum fine of R50 000,00 and/or imprisonment for maximum period of 2 years. These penalties are subject to the provision of the Adjustment of Fines Act 101 of 1991. She notes that the intention of the legislation is to provide that the maximum fine as an alternative to which a period of imprisonment may be imposed in respect of offences, shall be in the same ratio with regard to the period of imprisonment as the ratio of the fine as against imprisonment where the court is not a court of a Regional Division. She suggests that if the person has a licence to supply the equipment but does so to persons who do not have a licence to possess, the seller's licence may be revoked.

12.2.29.5 The Office of the Deputy Minister for Intelligence notes that their comments address the question whether the manufacture, distribution, possession and advertising of wire or oral communications interception devices should be regulated, and if so, how. They state that the above-mentioned activities by the private security industry, herein referred to as the industry, (this includes the private "intelligence" companies, and private investigators) are one of the main challenges facing the intelligence services, and they feel that the problem is broader than just manufacturing, distribution advertising and possession. They state that the problem extends to what they do with these devices, in light of the general prohibition imposed by the Interception and Monitoring Prohibition Act, 1992.

12.2.29.6 The Office of the Deputy Minister for Intelligence remarks that as the Commission is aware, the intelligence services have lodged a request with the Law Commission to assist with the review of security legislation and one of the aspect that has to be explored in this project is the activities of the industry. This is in light of section 199(3) of the Constitution, which provides for national legislation to be enacted to establish the services other than those established by the Constitution. They consider that, in light of the above, prohibition of some of the activities of this industry would therefore be unconstitutional.

12.2.29.7 The Office of the Deputy Minister for Intelligence consider that the security services may require the services of this industry - i.e. "manufacture and distribution" to the government security services. They point out that in order to deal with this problem one would suggest that the measures that were taken and the strategy that informed the regulation of foreign military assistance should be employed in order to deal with the activities of the industry. They point out that there should be registration by the industry, and only those who are registered in terms of the envisaged legislation which will be regulating the activities of the

industry should be allowed to manufacture, distribute, and possess these devices, for purposes of supplying the security services which are allowed by the Interception and Monitoring Prohibition Act to use those devices. They state that it is their opinion that this should be part of new legislation envisaged in paragraph 5 of the discussion paper and not as part of Act 127 as it is not the appropriate legislation to deal with these issues.

12.2.29.8 The Office of the Deputy Minister for Intelligence notes that the general prohibition in Act 127 should continue to apply to them, with the understanding that it is difficult to police until a separate legislation regulating the activities holistically is passed by parliament. They point out that the matter has policy implications, which require further discussion with the Security Ministers and the Joint Standing Committee on Intelligence and that any new ideas on the matter will be addressed before legislation is taken to Parliament.

12.2.29.9 Advocate Mnyatheli of the Investigating Directorate Serious Economic Offences remarks that in order to ensure strict compliance with the law prohibiting interception and/or monitoring other that in terms of the Statute it may important that regulations be put in place. He notes that according to the Act and the proposed amendment thereto activities of private investigators are unlawful and there is at the moment no effective control over them. He considers that consideration should be given very urgently to setting up systems and regulations for preventing unlawful interception and monitoring. Advocate Mnyatheli suggests that the first step towards this should be to control the manufacture and supply of wire, cable or oral communication interception devices. He considers that this will have the virtue of giving responsibility of control also to the manufacturers and distributors. He notes that the Telecommunications Act makes provision in terms of section 54 for use of telecommunications or radio equipment to be made only on the basis of prescribed regulations. He suggests that along similar lines perhaps, all of the above is achievable also by regulation. Advocate Mnyatheli considers that an unauthorized dealer, agent or private investigator cannot be expected to advertise for bugging services.

12.2.29.10 The SAPS[86] remarks that it is accepted that it will be difficult to define the devices in question and to enforce such a prohibition. The SAPS notes that ordinary micro-recorders or video cameras may be used or adapted to do surreptitious monitoring. They consider that

---

86 Chief Manager Legal Component Detective services.

what could maybe prohibited, is the possession of equipment designed or adapted to do surreptitious monitoring in suspicious circumstances along the lines of the prohibition on the possession of housebreaking equipment. The SAPS suggests that prohibition of the advertising of monitoring services which are unlawful, should be considered.

12.2.29.11 Judge Gordon remarks that business firms who advertise and practice prohibited acts or sell prohibited devices should be dealt with in the ordinary course by police action but only after written warnings to them to cease their activities. He considers that this would apply also, *mutatis mutandis* to the media advertising these acts. He considers that as proved overseas, it is extremely difficult to define precisely or effectively as to what constitutes a prohibited device. Judge Gordon notes that what has been accomplished under Army and Ammunition Acts cannot satisfactorily be accomplished in this case. He remarks that efforts may, of course, be made by experts of available devices to prescribe a suitable definition, or as close to one as possible, but that he leaves to the parties to decide.

12.2.29.12 Adv Molefe remarks that legislation against this faces the practical problem that it can have the effect of making the possession, manufacturing and distribution of items such as tape recorders, illegal. He considers that it is clear a serious technological input is required in order to classify these devices so that they can fall within a clear definition of what is prohibited. He considers that the ideal situation would be to legislate against highly specialised and sophisticated devices, to consider a permit or licence system in respect of less sophisticated or specialised devices, and to be totally silent on clearly less harmful devices such as tape recorders. Advocate Molefe remarks that generally, the law makes private bugging illegal. He considers that the use of private investigators is a reality of our times, especially in the business world. Given this scenario, he suggests judicial sanction here as well, but with even stricter control, criminal sanction and punitive measures where there is unauthorised intrusion or where the authorisation was obtained on the basis of false or dubious information. He considers that if those who indulge in this practice cannot be brought within the system then the same law must also make the practice of offering "bugging" services an offence.

12.2.29.13 Mr HP Rademeyer of the Department of Agriculture states that the Department does not have particular comments on the proposed amendments, it supports the principles contained in the proposed amendments and that the Department would like to see a stronger line being taken to curtail the proliferation of so-called "spy shops" and the uncontrolled use of

listening devices.

(b) Evaluation

12.2.29.14 Respondents were invited to advise the Commission on their views regarding the regulating of the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices. The Commission noted the comments by the office of the Deputy Minister of Intelligence which stated that this issue should be part of new legislation and not as part of Act 127 as it is not the appropriate legislation to deal with these issues, that the matter has policy implications, which require further discussion with the Security Ministers and the Joint Standing Committee on Intelligence and that any new ideas on the matter will be addressed before legislation is taken to Parliament. The Commission is of the view that the reasoning is persuasive.

(c) Recommendation

12.2.29.15 The Commission recommends that this aspect be dealt with in separate legislation. The Commission does therefore not make any recommendations for the inclusion in the Bill of provisions seeking to regulate the manufacture, distribution, possession and advertising of wire or oral communication intercepting devices.

12.2.30 Should the Act be more prescriptive?

(a) Comments on the proposed clause

12.2.30.1 The SAPS[87] notes that it should be remembered that the procedures in the Act have been working in practice since 1992. The SAPS points out that problems experienced in practice, as well as court cases did not reveal any shortcomings relating to the procedures. They note that procedures in the Act are further supplemented by the guidelines of the Judges-President, in respect of the manner and procedure of applications, provided for in section 6 of the Act. The SAPS points out that the provisions of section 6 at the same time provides some flexibility to amend and approve the procedures from time to time, without the necessity to

87 Chief Manager Legal Component Detective Services.

amend the Act.

12.2.30.2 The Director of Public Prosecutions Cape of Good Hope and the Office of the Director Investigating Directorate Organised crime and Public Safety remark as follows:

> Respondent wil ten sterkste aanbeveel dat die wet uiters voorskriftelik sal wees ten opsigte van ieder en elke handeling wat verrig word in verband met hierdie wet. Respondent is bewus daarvan dat daar 'n omvattende prosedure in Amerika aangewend word by die aanwending van hulle meeluisteringswet. So is daar byvoorbeeld bepalings dat indien monitoring deur een van die staatsinstansies gedoen word, die volgende prosedure gevolg moet word:
>
> a) Alle bandopnames moet twee bande hê en daar moet 'n sogenaamde 'slave tape" wees wat gebruik word vir ondersoekwerk en die eerste oorspronklike band wat saam met die sogenaamde "slave tape" opgeneem word moet onmiddellik verseël word en in veilige bewaring gehou word deur die betrokke instansie,
> b) Al hierdie betrokke bande wat opgeneem word tydens so 'n moniteringsproses moet gehou word en die praktyk wat tans in Suid-Afrika bestaan dat slegs relevante bande (in die diskresie van die ondersoekbeampte) gehou word moet mee weggedoen word.
> c) Hierdie bande word dan 'n periode van tien dae geneem na die betrokke regter wat die magtiging verleen en dan word hierdie bande in die teenwoordigheid van die regter geseël met die nodige amptelike seëls en dit word ex parte so op rekord geplaas.
> d) Hierdie band word dan in veilige bewaring gehou deur die regter se personeel of die regter kan gelas dat dit deur 'n sekere instansie op 'n bepaalde wyse in veilige bewaring gehou word.
>
> Die rede vir hierdie voorstel is dat daar groot onkostes aangegaan word om te bewys dat die bande wat deur die betrokke instansie opgeneem is die oorspronklike bande is en dat daar nie mee gepeuter is nie. Die ratio agter die hou van alle betrokke bande wat opgeneem word, is dat beskuldigdes nie later kan sê dat die bande wat wel gehou is, is uit konteks nie aangesien die bande wat wel vernietig is, die bande wat deur die Staat gehou is in konteks kan plaas nie.

12.2.30.3 Mr Mnyatheli of the Investigating Directorate Serious Economic Offences remarks that there is always some virtue to be gained in clarity especially in legal instruments, but the present position of the Act and the proposed amendment thereto is such that it is serviceable. Judicial pronouncements will always be necessitated by events and cases that come before the courts, that matter can hardly be avoided. He considers that on the other hand exhaustive detail can have its disadvantages and result in endless litigation.

12.2.30.4 Advocate Molefe remarks that without question the legislation needs to be

prescriptive. He notes that the Act justifies serious encroachment into human rights and economic freedom, and therefore must lay down strict procedures that have to be followed.

(b) Evaluation

12.2.30.5 It is clear from the comments noted above that the one assertion is that the statute under discussion is detailed enough, that exhaustive detail can have its disadvantages and result in endless litigation, whereas the opposing assertion is that since fundamental rights are encroached upon by this legislation, strict (and presumably detailed) procedures should be laid down in the Act.

12.2.30.6 The comment is noteworthy that a detailed procedure should be provided for in the Bill along the lines of the American legislation prescribing two sets of tapes when conversations are intercepted and monitored and how the tapes should be sealed and stored in order to overcome evidential problems. The Commission is not persuaded that detailed provisions should be included in the Bill seeking to regulate how interceptions of communications should be taped, sealed and stored. The Commission is of the view that it seems questionable whether the existing US provisions will solve all evidential problems concerning audio recordings. The Commission notes that there will be considerable financials implications if all recording devices were required to make an original and "slave tapes" simultaneously as the implementation of such a proposal will mean replacement of existing devices. The Commission is therefor of the view that there is no need for the Bill to be prescriptive on the way recording of communications or conversations should be conducted.

(c) Recommendation

12.2.30.7 The Commission recommends that there is no need to include detailed provisions in the Bill regulating how interceptions of communications should be recorded, sealed and stored in order to overcome potential evidential concerns.

12.2.31 Hacking

12.2.31.1 The Banking Council of South Africa states that it is intended to make it a criminal offence for anyone "intentionally and without the knowledge or permission of the

dispatcher (to intercept) a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line....". They suggest that the new legislation should also focus more specifically on the crime of computer systems "hacking". The Council notes that in many instances this involves illegal interception of legal transmissions over telecommunications networks, and in almost all cases telecommunication networks are used to perpetrate the crime. Messrs Sheer, De Wet, Van Schalkwyk, Wolmerans and Booysen of Obsidian Systems also address encryption and hacking in their submission. They remark that it is trivial for two parties to communicate using encrypted channels over the Internet and that such encryption software is freely available (at no cost and having essentially no copyright, patent, or licensing restrictions) on the Internet, and exists in strengths that make it absolutely impossible to eaves-drop on. They explain that this software is essential to the operation of many companies who use the software to provide security from computer vandals (hackers), industrial espionage and fraud, which would otherwise be impossible to prevent against or even to detect. They recommend that this issue be given substantial attention, to the extent perhaps of even drafting an entire Internet Communications Act. They consider that the Internet represents such a radical departure from traditional communications that it warrants a thorough investigation in itself.

12.2.31.2 The Commission considers that the matter of hacking and the broader issue of the desirability of legislation governing the Internet such as an Internet Communications Act should be dealt with in the Commission's investigation into computer related crimes (project 108) and not in this investigation.

12.2.32 Compliance with licence conditions and SATRA applying for orders to monitor and intercept

12.2.32.1 SATRA notes that section 35(4) of the Telecommunications Act provides that a licence shall be granted on such conditions appropriate to the licence. SATRA is of the opinion that, insofar as obligations of telecommunication service providers are concerned, it would be incumbent upon it to incorporate the obligations, as set out in paragraphs 14,15,16,17 and 19 as conditions in telecommunications licences that are issued should the obligations be passed into law. Other licence conditions such as a prohibition on provision of services that cannot be monitored could also be included in licences. SATRA licences would therefore reflect the security legislation and SATRA inspectors would be empowered in terms of Section 99 to take

the necessary steps, including the inspection of telecommunications equipment and facilities, to determine whether licence provisions incorporating conditions relating to monitoring are being complied with.

12.2.32.2 SATRA notes however that the proposed amendments will not entitle it to apply for orders that will authorise it to intercept and monitor telecommunications to determine whether the telecommunications are in breach of any of the provisions of the Telecommunications Act (eg the carrying of voice, the provision of a telecommunications service without a licence) or any licence issued in terms of the Telecommunications Act (which may include conditions relating to interception and monitoring). SATRA notes that the offence/breach may not be regarded as a "serious offence" within the meaning of the Act. SATRA remarks that as a statutory body, it is not entitled to rely on improperly obtained evidence to sanction persons in breach of the Telecommunications Act and/or their licence conditions. Thus SATRA argues that even though it is the regulatory body, in terms of current and proposed legislation, it has no legal means to intercept and monitor telecommunications.

12.2.32.3 The Commission initially considered that provision ought to be made in the Bill for the offences contemplated in sections 100[88] and 101[89] of the Telecommunications Act 103 of 1996 to be serious offences for purposes of the Interception and Monitoring Prohibition Act. This would mean that the South African Telecommunications Regulatory Authority (SATRA)

---

88 100(1): The Authority shall investigate and adjudicate-
(a) any alleged contravention of or failure by a licensee to comply with a provision of this Act, the relevant licence, any relevant agreement for the interconnection or provision of telecommunication facilities as contemplated in sections 43 and 44, respectively, or any direction in terms of section 36 (1) (d), 53 or 98;
(b) any failure by a provider of a telecommunication service to provide that service to or for any customer or end-user thereof, where such customer or end-user has, after complaint to the provider concerned, not obtained satisfaction.

89 101: A person shall be guilty of an offence if he or she-
(a) in making application for a licence, approval, certification or registration in terms of this Act, furnishes any false or misleading information or particulars or makes any statement which is false or misleading in any material respect, or wilfully fails to disclose any information or particulars material to his or her application;
(b) contravenes the provisions of section 30(1) (which regulates frequency and station licences, certificates and authorities), 31(1) (which regulates control of possession of radio apparatus), or 32(1) (prohibition on provision of telecommunication service without a licence); or
(c) contravenes any provision of section 99 (3); or
(d) fails, subject to section 100(4), to comply with any order made by the Authority in terms of section 100(3).

would be able to lay a charge with and request the SA Police Service to apply for a directive to authorise the interception and monitoring of telecommunications once SATRA inspectors have reasonable grounds to believe that telecommunication service providers are in breach of the provisions of the Telecommunications Act. The Commission however on reflection does not consider that such a provision would be appropriate in the light of the offences under discussion. The Commission further considers that the category of bodies who are presently empowered to apply for directives under the Interception Act, namely the SA Police Service, the National Defence Force, the Secret Service and the National Intelligence Agency should not be expanded to include the South African Telecommunications Regulatory Authority too.

12.2.33 Assistance in executing a directive

12.2.33.1 The SAPS[90] recommends that section 4 of the Act be amended to provide that any other person which has been authorized thereto, may execute or assist in the execution of a direction. The Act presently provides that any member of the Force as defined in section 1 of the South African Police Service Act, 1995 or a member, excluding a member of a visiting force, as defined in section 1 of the Defence Act, 1957 or a member of the Agency or the Service may execute a direction, provided that the member concerned has been authorized by the officer or member who made the application in terms of section 3 (2) to execute that direction or to assist with the execution of the direction. The SAPS notes that it has various civilian personnel who is not per definition a member as defined in section 1 of the South African Police Service Act, 1995, but who could, for instance, assist in the transcription of tapes. The Commission is of the view that the suggested amendment is a sensible addition to the Act.

12.2.33.2 The Commission recommends that section 4 of the Act be amended as follows:

> (1) If a directive has been issued in terms of section 3, any member of the Force as defined in section 1 of the South African Police Service Act, 1995 (Act 68 of 1995), or a member, excluding a member of a visiting force, as defined in section 1 of the Defence Act, 1957 (Act 44 of 1957), or a member of the Agency or the Service or any person may execute that directive, or assist with the execution of the directive concerned provided that the member or person concerned has been authorized by the officer or member who made the application in terms of section 3 (2) to execute that direction or to assist with the execution of the directive concerned.

---

90 Chief Manager Legal Component Detective Services.

12.2.34 Secrecy and empowering more persons to make applications under the Act

(a) Comments by respondents

12.2.34.1 Ms Naicker[91] suggests that a clause should be included in the legislation that deals directly with the conduct of the employees in the employ of a network provider. She suggests that the possession and/or distribution of intercepted information by employees of the Network Provider shall be an offence if the said information is disclosed to any person, body or organisation that is not authorised in terms of a Court issued directive, to have access to this information. She considers that a further duty is placed on the Network provider to include in the contract of employment a secrecy clause, which binds the employee not to disclose any information to unauthorised persons. She suggests that the failure to abide by the secrecy clause would result in termination of the employee's services on the grounds of a breach of trust.

12.2.34.2 Ms Naicker suggests that a useful clause would be one which allows the Ministers of various Departments to make applications to monitor situations which are relevant to their respective Departments namely where organised fraud is taking place within the Department by State officials. This will facilitate the investigation and subsequent prosecution of corrupt State officials. She remarks that the monitoring should be done within the confines of the Act and the crimes which are stipulated in the Act.

12.2.34.3 Ms Naicker notes that the Office of President ought to be vested with a right to make an application for the interception and monitoring of any and all State Departments within the confines of the Act. She considers that this section should serve as a safety measure for serious offences committed at ministerial level and shall include the interception and monitoring of the SAPS, NIA, SASS and SANDF, should it be necessary. She proposes that the Office of the President may then co-opt the services of any of the four aforesaid State Departments in order to facilitate the monitoring on a technical and administrative level. Mr Harold Marshall proposed that consideration be given that applications by registered, qualified or listed private investigators should also be considered. He argues that due to the workload at present, the SA Police may not have the manpower to handle an investigation and that, at this time, many

---

91 Of the Department of Public Works.

companies are using private investigators to obtain all the evidence required for a conviction. He explains that the case is only then handed to the Police and a case is opened for prosecution and possibly, with the approval of a Branch Commander or similar rank, an application can be made and approved for private investigators to carry out the surveillance and monitoring. He suggests that bona fide private investigation companies should apply to be on an approved list and that this will help to eliminate 'fly-by-night' detectives.

(b) Evaluation

12.2.34.4 The Commission is of the view that the proposal for vesting the Office of the President and registered, qualified or listed private investigators with a right to make applications under the Act is not persuasive.

(c) Recommendation

12.2.34.5 The Commission considers that the position should remain as set out in the Act, which entitles only the SA Police Service, the National Defence Force, the Secret Service and the National Intelligence Agency to make applications under the Act.

12.2.35 Making provision for telecommunication service provider employees to answer directives by way of affidavit

(a) Proposals by respondents

12.2.35.1 MTN is of the opinion that, due to the sensitive nature of the information, MTN be allowed to answer the directives by way of affidavit. Furthermore MTN submits that to protect its employees a structure should be created in the event of any judicial proceeding whereby the aforementioned affidavit will be used in such proceedings and MTN employees will not be required to testify in Court. Vodacom remarks that it wishes to register the need for statutory protection for employees of telecommunication service operators involved in activities relating to the implementation of the Act, such as evidence be given by means of affidavit. Vodacom considers that, given the potential for violence against, and for intimidation of, employees routinely involved in the implementation of the Act, the possibility be investigated of a special procedure whereby any required cross-examination could be carried out in a

manner which preserves the secrecy of the identity of those network employees. Vodacom states that given the potential high frequency of requests for information and of criminal proceedings in terms of the Act and other Acts, these procedures are also required to prevent an unnecessary loss of man-hours and productivity.

(b) Evaluation

12.2.35.2 This proposal means the enactment of a provision similar to section 212 of the Criminal Procedure Act. The effect of this provision is that an affidavit of an official constitutes on its mere production at criminal proceedings prima facie proof that a certain transaction or occurrence in a state department, provincial department, court of law or bank did take place, that information or a document allegedly supplied to him or her was not supplied and that he or her has carried out certain executive powers conferred by law to him or her and who has himself or herself carried out those powers or satisfied himself or herself that such powers have duly been carried out. The provision further provides that the court before which an affidavit or certificate is produced as *prima facie* proof of the relevant contents thereof, may in its discretion cause the person who made the affidavit or issued the certificate to be subpoenaed to give oral evidence in the proceedings in question, or may cause written interrogatories to be submitted to such person for reply, and such interrogatories and any reply thereto purporting to be a reply from such person, shall likewise be admissible in evidence at such proceedings. It is apparent that MTN's intention with the proposed clause is to "protect" their employees from testifying in court. Whenever the information set out in an affidavit is in dispute, the employee of the service provider will necessarily have to testify in court. Hence, the proposed provision will not prevent these employees from having to attend court proceedings.

(c) Recommendation

12.2.35.3 The Commission is of the view that there is no need to confer the proposed power to officials employed by telecommunication service providers to answer directives by way of affidavit.

12.2.36 Indemnify licenced telecommunications operators from claims where they act in accordance with a *prima facie* directive

12.2.36.1 MTN suggests that MTN and any licenced telecommunications operator be indemnified from any claims where MTN acted in accordance with a *prima facie* written directive. Vodacom suggests that in the light of the high level of intrusion into an individual's privacy, and the concomitant possibility of prosecution for violating the terms of the Act as well as claims for damages by individuals against the State and network operators, an indemnity clause should be added to the Act. Vodacom proposes that a network operator and its employees should be indemnified against criminal prosecution or a claim for damages, where the company and employees have acted in good faith and in the normal execution of its statutory obligations in terms of the Act.

12.2.36.2 The Commission is of the view that the Bill ought to make provision for circumstances where a person intercepted or monitored communications in good faith or assisted another in good faith in monitoring or intercepting communications, in the belief that the interception or monitoring was being undertaken in accordance with a duly authorised directive. The Commission therefore recommends that a person who intercepts or monitors a communication in accordance with a directive or who in good faith assists a person who her or she believes on reasonable grounds is acting in accordance with a directive, should not be guilty of an offence.

12.2.37 Written directives should be served upon telecommunication service providers at a central point

12.2.37.3 MTN submits its preference to written directives being served upon MTN at a central point in order for effect to be given to the purport of this particular Bill. Vodacom notes that, given the unavoidable limitations on technological and administrative capacity, it is imperative that each judge in a division maintains a list for each operator, indicating the priority of execution of all currently active directives. Vodacom considers that networks cannot be expected to decide between various directives issued at various points which end up competing for limited resources, especially given the severe penalty provisions which are proposed. Vodacom also considers that directives be served on operators at a central point agreed upon between the members of the state agencies and each network operator. Vodacom is of the view that this will ensure accountability, the effective and co-ordinated implementation and management of the system, and proposes the addition of the following clauses to section 3(1):

(a) and which direction shall indicate the priority of execution in the case of more than one active directive applicable to a specific telecommunication service operator;

(b) which directive, in the case of a telecommunication service operator, shall be served on the telecommunication service operator at a central point, as agreed upon with the telecommunications operator.

12.2.37.2 The Commission considers that this is a matter which should be negotiated between telecommunication service providers and the parties involved in executing directives. The Commission is of the view that there is no need to seek to regulate this aspect in the proposed Bill.

ANNEXURE "A"

INTERCEPTION AND MONITORING PROHIBITION AMENDMENT BILL, 1999

BILL

To amend the Interception and Monitoring Prohibition Act, 1992, so as to prohibit the provision of telecommunication services which are not capable of being monitored, to make further provision for consideration of applications, to regulate the monitoring in terms of this Act of communications; to amend the Criminal Procedure Act, 1977, so as to further regulate the giving of information as to any alleged offence; to amend the Drugs and drug Trafficking Act, 1996, so as to further regulate the delivery or submitting of registers, records or documents which may have a bearing on alleged offences under the Act to a police official; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:-

Amendment of section 1 of Act 127 of 1992, as amended by section 32 of Act 38 of 1994, section 1 of Act 77 of 1995 and section 13 of Act 34 of 1998

1. Section 1 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended -

(a) by the insertion, after the definition of "agency" of the following definition:

"'call-related information' includes switching, dialling or signalling information that identifies the origin, destination, termination, duration and equipment identification of each communication generated or received by a customer or user of any equipment, facility or service rendered by a person, body or organization rendering a telecommunication service, and where applicable the location of the user at the time of the initiation or first reception of a call."

(b) by the insertion, after the definition of "agency" of the following definition:

"'communication' includes conversation and a message, and any part of a conversation or message, whether:
(a) in the form of:

(i) speech, music or other sounds;
(ii) data;
(iii) text;
(iv) visual images, whether or not animated; or
(v) signals; or

(b) in any other form or in any combination of forms.

(c) by the deletion of the definition of "division":

['division' means a provincial or local division of the Supreme Court of South Africa];

(d) by the substitution for the definition of "judge" of the following definition:

"'judge' means any judge of any provincial or local division of the **[Supreme]** High Court of South Africa, including any judge discharged from active service under section 3 of the Judges' Remuneration and Conditions of Employment Act, 1989 (Act No 88 of 1989), and any retired judge, who is designated by the Minister of Justice to perform the functions of a judge **[within a particular division]** for the purposes of this Act."

(e) by the substitution for the definition of "monitor" of the following definition:

"'monitor' includes the recording of **[conversations or]** communications by means of a monitoring device;"

(f) by the substitution for the definition of "monitoring device" of the following definition:

"'monitoring device' means any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any **[conversation or]** communication;"

(g) by the substitution for the definition of "serious offence" of the following definition:

"'serious offence' means -

(a) any offence mentioned in Schedule I to the Criminal Procedure Act, 1977 (Act No. 51 of 1977), **[including any conspiracy, incitement or attempt to commit any offence referred to in that Schedule,]** provided that -

[(i) **that offence is allegedly being or has allegedly been committed over a lengthy period of time]**;

[(ii)] (i) that offence is allegedly being or has allegedly been committed on an organized, planned or premeditated basis **[by the persons involved therein]**; or

[(iii)] (ii) that offence is allegedly being or has been committed on

a regular basis **[by the person or persons involved therein]**; or

[(iv)](iii) that offence may allegedly harm the economy or other compelling national interests of the Republic; or

(b) any offence referred to in sections 13 (f) and 14 (b) of the Drugs and Drug Trafficking Act, 1992; or

(c) any offence relating to the trafficking in firearms, ammunition and explosives; or

(d) any offence relating to the death or serious bodily harm of any person; or

(e) any offence referred to in the Prevention of Organized Crime Act, 1998, or

(f) any offence threatening the security of the Republic;

including any conspiracy, incitement or attempt to commit any of the above-mentioned offences."

(h) by the substitution for the definition of "telecommunications line", of the following definition:

"**['telecommunications line' includes any apparatus, instrument, pole, mast, wire, pipe, pneumatic or other tube, thing or means which is or may be used for or in connection with the sending, conveying, transmitting or receiving of signs, signals, sounds, communications or other information]** 'telecommunications system' means any system or series of telecommunication facilities or radio, optical or other electromagnetic apparatus or any similar technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to rearrangement, composition or other processes by any means in the course of their transmission or emission or reception;";

(i) by the insertion, after the definition of "telecommunications line", of the following definition:

"'telecommunication service' means any telecommunication service as defined in the Telecommunications Act, 1996 (Act No. 103 of 1996), in respect of -

(a) a public switched telecommunication service;

(b) a mobile cellular telecommunication service;

(c) a national long distance telecommunication service;

(d) an international telecommunication service; or

(e) any other telecommunication service licensed or deemed to be licensed or exempted from being licensed as such in terms of the Telecommunications Act, 1996;"

(j) 'telegram' means any communication in written form or information in the form of an image transmitted over a communications line and delivered in any such form, or intended to be thus transmitted and delivered, or delivered from any post office as defined in the Post Office Act, 1958 (Act 44 of 1958), or intended to be thus delivered as a communication or as information transmitted either wholly or in part over a telecommunications **[line]** system.

Amendment of section 2 of Act 127 of 1992, as amended by section 14 of Act 34 of 1998

2. Section 2 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended-

(a) by the substitution for subsection (1) of the following subsection:

"1. Save as is provided in section 3, **[N]** no person shall-
(a) intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications **[line]** system; or
(b) intentionally monitor any **[conversation or]** communication by means of a monitoring device so as to gather confidential information concerning any person, body or organization;"

(b) by the substitution for subsection (2) of the following subsection:

"(2) Notwithstanding the provisions of subsection (1) or anything to the contrary in any other law contained, a judge may direct that-
(a) a particular postal article or a particular communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications **[line]** system be intercepted;
(b) all postal articles to or from a person, body or organization or all communications which have been or are being or are intended to be transmitted by telephone or in any other manner over a telecommunications **[line]** system, to or from a person, body or organization be intercepted; or
(c) **[conversations by or with, or]** communications to or from, a person, body or organization, whether a telecommunications **[line]** system is being used in conducting **[those conversations]** or transmitting those communications or not, be monitored in any manner by means of a monitoring device."

Amendment of section 3 of Act 127 of 1992, as amended by section 32 of Act 38 of 1994, section 4 of Act 18 of 1996, and section 15 of Act 34 of 1998

3. Section 3 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended by -

(a) the substitution for subsection (1) of the following subsection:

"(1) A **[direction]** directive referred to in section 2 (2) may only be issued by a judge-
[(a) designated by the Minister of Justice for the Division -
(i) from where the postal article or communication referred to in section 2(2)(a) or (b) has been or will probably be dispatched or transmitted or where that postal article or communication will probably be received; or
[(ii) where the proposed monitoring referred to in section 2(2)(c)

will be carried out; and

(b)] if the judge is **[convinced]** satisfied, on the **[grounds mentioned]** facts alleged in a written application that complies with the directives referred to in section 6 that there are reasonable grounds to believe that-

(a) **[that]** the offence that has been or is being or will probably be committed, is a serious offence that cannot be **[properly]** investigated in **[any other]** another appropriate manner **[and of which the investigation in terms of this Act is necessary]**; or

(b) **[that]** the security or other compelling national interests of the Republic **[is]** are threatened or that the gathering of information concerning a threat to the security or other compelling national interests of the Republic is necessary";

(b) the substitution for subsection (2) of the following subsection:

"(2) An application shall-

(a) for the purposes referred to in subsection (1) **[(b)(i)]** (a) or **[(ii)]** (b) or subsection (4), be made by an officer referred to in section 33 of the South African Police Service Act, 1995 (Act 68 of 1995), provided the officer concerned obtained in advance the approval of another officer in the South African Police Service with at least the rank of assistant-commissioner, or a member of the said Police Service occupying a post on at least the same level, and who has been authorised in writing by the National Commissioner of the South African Police Service to grant such approval;

(b) for the purposes of subsection (1)(b) **[(ii)]** or subsection (4), be made by an officer as defined in section 1 of the Defence Act, 1957 (Act 44 of 1957), provided that the officer concerned obtained in advance the approval of another officer in the South African National Defence Force with at least the rank of major-general who shall be authorized in writing by the Chief of the South African National Defence Force to grant such approval; or

(c) for the purposes of subsection (1)(b) **[(ii)]** or subsection (4), be made by a member as defined in section 1 of the Intelligence Services Act, 1994, provided the member concerned obtained in advance the approval of another member of the Agency or Service, as the case may be, holding a post of at least chief director."

(c) by the substitution for subsection (3) of the following subsection:

"(3) A **[direction]** directive referred to in section 2 (2) shall be issued by the judge concerned for a period not exceeding three months at a time, and the period for which it has been issued shall be mentioned in the **[direction]** directive."

(d) the substitution for subsection (5) of the following subsection:

"(5) An application referred to in subsection (1)**[(b)(i)]** (a) or **[(ii)]** (b) or subsection (4) shall be heard and a **[direction]** directive issued without any notice to the person, body or organization to which the application applies and without hearing such person, body or organization."

(e) the substitution for subsection (6) of the following subsection:

"(6) An application referred to in subsection (1)**[(b)(i)]** (a) or **[ii]** (b) or subsection (4) may also be granted if an investigation in terms of this Act may disclose information that may contribute to preventing the perpetration of a serious offence."

(f) the insertion of the following subsection:

"(7) No communication between a legal representative and his or her client may be intercepted or monitored, except if on reasonable grounds, the judge is satisfied that such a legal representative is involved in, or aiding or abetting a serious offence or an offence threatening the security of the Republic."

(g) the insertion of the following subsection:

"(8) The judge referred to in subsection (1) may, upon application that complies with the directives referred to in section 6, direct further additions or amendments to an existing directive referred to in section 2(2) if the judge is satisfied that the addition or amendment is necessary for a reason referred to in subsection (1)(a) or (b). "

Amendment of section 4 of Act 127 of 1992, as amended by section 32(1) of Act 38 of 1994 and section 4 of Act 18 of 1996

4. Section 4 of Act 127 of 1992, is hereby amended-

(a) by the substitution for subsection (1) of the following subsection:

"(1) If a **[direction]** directive has been issued in terms of section 3, any member of the Force as defined in section 1 of the South African Police Service Act, 1995 (Act 68 of 1995), or a member, excluding a member of a visiting force, as defined in section 1 of the Defence Act, 1957 (Act 44 of 1957), or a member of the Agency or the Service, or any other person may execute that **[direction]** directive or assist with the execution of the directive concerned, provided that the member or person concerned has been authorized by the officer or member who made the application in terms of section 3(2) to execute that **[direction]** directive or to assist with the execution of the **[direction]** directive concerned."

(b) by the substitution for subsection (2) of the following subsection:

"(2) A member who executes a **[direction]** directive or assists with the execution of a **[direction]** directive may-

(a) take possession of and examine any postal article or telegram to which the **[direction]** directive applies, or as the case may be, listen in to or make a recording of any **[conversation or]** communication to which the **[direction]** directive applies;"

(c) by the substitution for subsection (3) of the following subsection:

"(3) The officer or member who granted the authorization referred to in subsection (1), may authorize such number of members to assist with the execution of the **[direction]** directive as he or she deems necessary."

(d) by the substitution for subsection (4) of the following subsection:

"(4) A member who executes a **[direction]** directive or assists with the execution of a **[direction]** directive may at any time enter upon any premises in order to install, maintain or remove a monitoring device, or to intercept or take into possession a postal article, or to intercept any communication, or to install, maintain or remove a device by means of which any communication can be intercepted, for the purposes of this Act."

Amendment of section 5 of Act 127 of 1992, as amended by section 32 of Act 38 of 1996, section 4 of Act 18 of 1996 and section 17 of Act 34 of 1998

5. Section 5 of Act 127 of 1992, is hereby amended-

(a) by the substitution for subsection (1) of the following section:

"(1) If a **[direction]** directive referred to in section 2 (2) or a copy thereof is handed to the person or organization **[who is]** responsible for the dispatching of a postal article or the transmission of a communication over a telecommunications [**line**] system, or for the rendering of a postal service or telecommunication service, to a person, body or organization mentioned in that **[direction]** directive by a member who executes that **[direction]** directive or assists with the execution of that **[direction]** directive, the person, body or organization concerned shall as soon as possible-

(a) intercept the postal article or telegram concerned or all postal articles or telegrams to which the **[direction]** directive applies and hand it or them over to a member who is authorized in terms of section 4(1) to execute the **[direction]** directive concerned or to assist with the execution thereof;

(b) make available the necessary facilities and devices and enable the member who is authorized in terms of section 4(1) to execute a **[direction]** directive or to assist with the execution of a **[direction]** directive, to effect the necessary connections in order to monitor

[conversations or] communications to which the **[direction]** directive applies."

(b) by the substitution for subsection (2) of the following subsection:

"(2) If a person, body or organization has made a facility, device or telecommunications **[line]** system available for the purposes mentioned in subsection (1) (b), the remuneration agreed upon by the person or organization and the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force or the Director-General of the Agency or the Service, as the case may be, shall be paid to that person, body or organization."

(c) by the insertion of a new subsection (4) -

"(4) The remuneration referred to in subsections (2) and (3) shall only be in respect of direct costs incurred in respect of personnel and administration and the lease of telecommunications systems, where applicable, and shall not include the costs of acquiring the facilities and devices referred to section 5A(2)."

Insertion of sections 5A and 5B in Act 127 of 1992

6. The following sections are hereby inserted after section 5 of the Interception and Monitoring Prohibition Act, 1992 -

Prohibition on certain telecommunications services:
5A(1) Notwithstanding the provisions of any other law, no person, body or organization rendering a telecommunication service, may provide any such service which does not have the capacity to be monitored: Provided that the person, body or organization rendering such a service shall not be responsible for decrypting any communication encrypted by the customer contracted for the use of the service, unless the facility for encryption was provided by the body, person or organization rendering the service.

(2) Any person, body or organization rendering a telecommunication service shall at own cost and within the period specified by the Minister for Posts, Telecommunications and Broadcasting, in a directive referred to in subsection (6), acquire the necessary facilities and devices to enable the monitoring of communications.

(3) The investment, technical, maintenance and operating costs in enabling a telecommunication service to be monitored, shall be carried by the person, body or organization rendering such a service.

(4) Duplicate signals of communications authorized to be monitored in terms of this Act, shall be routed by the relevant person, body or organization rendering a telecommunication service to the relevant central monitoring centre, to be designated by, respectively, the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force, and the Directors-General of the Agency and Service.

(5) The South African Police Service, the South African National Defence Force, the Agency and the Service shall, at State expense, equip, operate and maintain central monitoring centres for the authorized monitoring of communications: Provided that an agreement on the sharing of any such central monitoring centre shall not be excluded.

(6) The Minister for Posts, Telecommunications and Broadcasting, after consultation with any person, body or organization rendering a telecommunication service, may issue a directive to comply with subsection (1) and may, in such directive, specify the security, technical and functional requirements of the facilities and devices to be acquired in terms of subsection (2).

(7) The directives referred to in subsection (6) may include, but are not limited, to specifications on the following -

(a) the capacity needed for interception purposes;
(b) systems to be used;
(c) connectivity with designated central monitoring centres;
(d) the manner of transmission of duplicated signals of communications to be intercepted, to the designated central monitoring centres referred to in subsection (5); or
(e) the manner of transmission of call-related information to the central monitoring centres, referred to in section 5B.

(8) The Minister for Posts, Telecommunications and Broadcasting after consultation with any person, body or organization rendering a telecommunication service, may determine a period, which shall not be less than three months from the date on which a directive in terms of subsection (6) is issued, for compliance with such a directive.

Call-related information

5B(1) Any person who is authorized to apply for a directive referred to in section 2(2), may also apply, in the manner prescribed in this Act, for a supplementary directive for the provision on an ongoing basis for a specified duration, of call-related information, as it becomes available.

(2) Any person, body or organization rendering a telecommunication service shall, in respect of all communications which are monitored in terms of this Act, route the call-related information specified in a supplementary directive referred to in subsection (1) to the relevant designated central monitoring centre.

(3) If, in a specific case, only call-related information is required on an ongoing basis without the actual monitoring of the communication in question, the judge may direct that the relevant person, body or organization rendering a telecommunication service to whom or which a directive is addressed, provide such call-related information to the South African Police Service, the South African National Defence Force, the Agency or the Service, whichever is applicable.

(4) The availability of the above procedures in respect of the ongoing provision of call-related information excludes the use of any power in any other Act, to obtain evidence or information in respect of a person, body or organization, notwithstanding anything to the contrary in any other Act.

(5) Any person, body or organization rendering a telecommunication service shall -

(a) ensure that proper records regarding identities and addresses are kept in respect of clients to whom a telecommunication service is contracted, whether on a prepaid or contract basis;

(b) require positive identification from a client to whom such a service is contracted.

(6) Any person, body or organization rendering a telecommunication service, shall provide such information regarding the customer who has contracted for the use of such telecommunication service to the South African Police Service, the South African National Defence Force, the Agency or the Service, as may be required by an officer or member referred to in section 3(2)(a), (b) and (c) to fulfil the functions and exercise the powers authorized by law.

(7) The obligation in terms of subsection (5) includes the provision of the name, identity number and address of the person contracted for the use of a specific telecommunications number.

Amendment of section 6 of Act 127 of 1992

7. Section 6 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended by the insertion of the following subsection:

"(2) If the judge referred to in subsection 3(1)(a) considers any case to be sufficiently urgent, the procedure contemplated in subsection (1) may be dispensed with and the matter may be dealt with in such manner and subject to such conditions as the judge may deem fit, including the grant in any appropriate case of an oral directive followed up by a written application incorporating the terms of the directive within one week: Provided that where an oral directive is issued, the judge shall reduce it to writing within two days.".

Insertion of section 6A in Act 127 of 1992

8. The following section 6A is hereby inserted in the Interception and Monitoring Prohibition Act, 1992, after section 6:

"6A(1) The use of any information obtained through the application of this Act, or any similar Act in another country, as evidence in any prosecution, is subject to the decision of the Director of Public Prosecutions or an Investigating Director contemplated in the National Prosecuting Authority Act, 1998 (Act No 32 of 1998)."

"(2) Information regarding the commission of any criminal offence, obtained by means of any interception or monitoring in terms of this Act, or any similar Act in another country, may be admissible as evidence in criminal proceedings."

Amendment of section 8 of Act 127 of 1992

9. Section 8 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended

(a) by the insertion of the following subsection:

"(3) Any person who intercepts or monitors a communication in accordance with a directive issued under this Act or who in good faith assists a person who he or she believes on reasonable grounds is acting in accordance with a directive, is not guilty of an offence."

(b) by the insertion of the following subsection:

"(1A) Any person, body or organization rendering a telecommunication service and failing or refusing to comply with -

(a) a directive issued by a judge in terms of section 2(2) or 5B(2);

(b) a directive issued by the Minister for Posts, Telecommunications and Broadcasting in terms of section 5A(7);

(c) the obligation in terms of section 5B(6) to provide information regarding a user of a telecommunication service; or

(d) the obligation in terms of section 5B(5)(a) to keep the records referred to in that section; or

(e) the obligation in terms of section 5B(5)(b) to require positive identification when contracting a telecommunication service;

shall be guilty of an offence, and liable on conviction, to a fine not exceeding R 200 000."

Insertion of section 8A into Act 127 of 1992

10. The Interception and Monitoring Prohibition Act, 1992, is hereby amended by the insertion of the following section:

"8A. If any person, body or organization rendering a telecommunication service, fails, after a conviction for failing to comply with a directive issued in terms of section 5A(6), to comply with a further such directive, the Minister for Posts, Telecommunications and Broadcasting may revoke the licence issued in terms of Chapter V of the Telecommunications Act, 1996, to such person, body or organization to render a telecommunication service.

Transitional arrangements

11. All directives which have been issued by a judge in terms of the Interception and Monitoring Prohibition Act, 1992, when this Act comes into operation, shall remain in force and, unless extended by a judge in terms of section 3, expire on the date determined in the directive.

Substitution of long title of Act 127 of 1992

12. The following long title is hereby substituted for the long title of the Interception and Monitoring Prohibition Act, 1992:

"ACT

To prohibit the interception of certain communications and the monitoring of certain **[conversations or]** communications, to prohibit the rendering of certain telecommunication services which do not have the capacity to be monitored, to regulate authorised telecommunications monitoring; to provide for the interception of postal

articles and communications in the case of a serious offence or if the security of the Republic is threatened; and to provide for matters connected therewith."

Amendment of section 205 of Act 51 of 1977

13. Section 205 of the Criminal Procedure Act, 1977, is hereby amended by the substitution for subsection (1) of the following subsection:

(1) A judge of the Supreme Court, a regional court magistrate or a magistrate may, subject to the provisions of subsection 4, and the provisions of section 5B(4) of the Interception and Monitoring Prohibition Act, 1999, upon the request of an attorney-general or a public prosecutor authorized thereto in writing by the attorney-general, require the attendance before him or any other judge, regional court magistrate or magistrate, for examination by the attorney-general or the public prosecutor authorized thereto in writing by the attorney-general, of any person who is likely to give material or relevant information as to any alleged offence, whether or not it is known by whom the offence was committed: Provided that if such person furnishes that information to the satisfaction of the attorney-general or public prosecutor concerned prior to the date on which he is required to appear before a judge, regional court magistrate or magistrate, he shall be under no further obligation to appear before a judge, regional court magistrate or magistrate.

Amendment of section 11 of Act 140 of 1992

14. Section 11 of the Drugs and Drug Trafficking Act, 1992 is hereby amended by the substitution for paragraph (e) of subsection (1) of the following paragraph:

(e) subject to the provisions of section 5B(4) of the Interception and Monitoring Prohibition Act, 1999, require from any person who has in his possession or custody or under his control any register, record or other document which in the opinion of the police official may have a bearing on any offence or alleged offence under this Act, to deliver to him then and there, or to submit to him at such time and place as may be determined by the police official, any such register, record or document;

15. Short title and commencement

7(1) This Act shall be called the Interception and Monitoring Prohibition Amendment Act, 1999.

(2) This Act shall come into operation on a date fixed by the President by Proclamation in the Gazette.

ANNEXURE B

THE INTERCEPTION AND MONITORING PROHIBITION ACT 127 OF 1992

[ASSENTED TO 2 JULY 1992] [DATE OF COMMENCEMENT: 1 FEBRUARY 1993]

ACT

To prohibit the interception of certain communications and the monitoring of certain conversations or communications; to provide for the interception of postal articles and communications and for the monitoring of conversations or communications in the case of a serious offence or if the security of the Republic is threatened; and to provide for matters connected therewith.

1 Definitions

In this Act, unless the context otherwise indicates-

'Agency' means the Agency as defined in section 1 of the Intelligence Services Act, 1994;

'division' [means] a provincial or local division of the Supreme Court of South Africa;

'judge' means any judge of any provincial or local division of the Supreme Court of South Africa including any judge discharged from active service under section 3 of the Judges' Remuneration and Conditions of Employment Act, 1989 (Act 88 of 1989), and any retired judge, who is designated by the Minister of Justice to perform the functions of a judge within a particular division for the purposes of this Act;

'monitor' includes the recording of conversations or communications by means of a monitoring device;

'monitoring device' means any instrument, device or equipment which is used or can be used, whether by itself or in combination with any other instrument, device or equipment, to listen to or record any conversation or communication;

'postal article' means any letter, post-card, reply post-card, letter-card, newspaper, book, packet, pattern or sample packet or any parcel or other article while in transit by post, and includes a telegram when conveyed by post;

'serious offence' means-

(a) any offence mentioned in Schedule 1 to the Criminal Procedure Act, 1977 (Act 51 of 1977), including any conspiracy, incitement or attempt to commit any offence referred to in that Schedule, provided that-

(i) that offence is allegedly being or has allegedly been committed over a lengthy period of time;

(ii) that offence is allegedly being or has allegedly been committed on an

organized basis by the persons involved therein;

(iii) that offence is allegedly being or has allegedly been committed on a regular basis by the person or persons involved therein; or

(iv) that offence may allegedly harm the economy of the Republic; or

(b) any offence referred to in sections 13 (f) and 14 (b) of the Drugs and Drug Trafficking Act, 1992;

'Service' means the Service as defined in section 1 of the Intelligence Services Act, 1994;

'telecommunications line' includes any apparatus, instrument, pole, mast, wire, pipe, pneumatic or other tube, thing or means which is or may be used for or in connection with the sending, conveying, transmitting or receiving of signs, signals, sounds, communications or other information;

'telegram' means any communication in written form or information in the form of an image transmitted over a communications line and delivered in any such form, or intended to be thus transmitted and delivered, or delivered from any post office as defined in the Post Office Act, 1958 (Act 44 of 1958), or intended to be thus delivered as a communication or as information transmitted either wholly or in part over a telecommunications line.

2 Prohibition on interception and monitoring

(1) No person shall-

(a) intentionally and without the knowledge or permission of the dispatcher intercept a communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line; or

(b) intentionally monitor any conversation or communication by means of a monitoring device so as to gather confidential information concerning any person, body or organization.

(2) Notwithstanding the provisions of subsection (1) or anything to the contrary in any other law contained, a judge may direct that-

(a) a particular postal article or a particular communication which has been or is being or is intended to be transmitted by telephone or in any other manner over a telecommunications line be intercepted;

(b) all postal articles to or from a person, body or organization or all communications which have been or are being or are intended to be transmitted by telephone or in any other manner over a telecommunications line, to or from a person, body or organization be intercepted; or

(c) conversations by or with, or communications to or from, a person, body or organization, whether a telecommunications line is being used in conducting those conversations or transmitting those communications or not, be monitored in any manner by means of a monitoring device.

3 Issue of directive

(1) A direction referred to in section 2 (2) may only be issued by a judge-

(a) designated by the Minister of Justice for the division-

(i) from where the postal article or communication referred to in section 2 (2) (a) or (b) has been or will probably be dispatched or transmitted or where that postal article or communication will probably be received; or

(ii) where the proposed monitoring referred to in section 2 (2) (c) will be carried out; and

(b) if the judge concerned is convinced, on the grounds mentioned in a written application that complies with the directives referred to in section 6 -

(i) that the offence that has been or is being or will probably be committed, is a serious offence that cannot be properly investigated in any other manner and of which the investigation in terms of this Act is necessary; or

(ii) that the security of the Republic is threatened or that the gathering of information concerning a threat to the security of the Republic is necessary.

(2) An application shall-

(a) for the purposes referred to in subsection (1) (b) (i) or (ii) or subsection (4), be made by an officer referred to in section 33 of the South African Police Service Act, 1995 (Act 68 of 1995), provided the officer concerned obtained in advance the approval of another officer in the South African Police Service with at least the rank of assistant-commissioner, or a member of the said Police Service occupying a post on at least the same level, and who has been authorised in writing by the National Commissioner of the South African Police Service to grant such approval;

(b) for the purposes of subsection (1) (b) (ii) or subsection (4), be made by an officer as defined in section 1 of the Defence Act, 1957 (Act 44 of 1957), provided that the officer concerned obtained in advance the approval of another officer in the South African National Defence Force with at least the rank of major-general who shall be authorized in writing by the Chief of the South African National Defence Force to grant such

approval; or

(c) for the purposes of subsection (1) (b) (ii) or subsection (4), be made by a member as defined in section 1 of the Intelligence Services Act, 1994, provided the member concerned obtained in advance the approval of another member of the Agency or Service, as the case may be, holding a post of at least chief director.

(3) A direction referred to in section 2 (2) shall be issued by the judge concerned for a period not exceeding three months at a time, and the period for which it has been issued shall be mentioned in the direction.

(4) The judge referred to in subsection (1) may, upon an application that complies with the directives referred to in section 6, extend the period referred to in subsection (3) for a further period not exceeding three months at a time if that judge is convinced that the extension is necessary for a reason mentioned in subsection (1) (b) (i) or (ii).

(5) An application referred to in subsection (1) (b) (i) or (ii) or subsection (4) shall be heard and a direction issued without any notice to the person, body or organization to which the application applies and without hearing such person, body or organization.

(6) An application referred to in subsection (1) (b) (i) or (ii) or subsection (4) may also be granted if an investigation in terms of this Act may disclose information that may contribute to preventing the perpetration of a serious offence.

4 Execution of direction

(1) If a direction has been issued in terms of section 3, any member of the Force as defined in section 1 of the South African Police Service Act, 1995 (Act 68 of 1995), or a member, excluding a member of a visiting force, as defined in section 1 of the Defence Act, 1957 (Act 44 of 1957), or a member of the Agency or the Service may execute that direction, provided that the member concerned has been authorized by the officer or member who made the application in terms of section 3 (2) to execute that direction or to assist with the execution of the direction concerned.

(2) A member who executes a direction or assists with the execution of a direction may-

(a) take possession of and examine any postal article or telegram to which the direction applies, or as the case may be, listen in to or make a recording of any conversation or communication to which the direction applies;

(b) return a postal article or telegram that was taken into possession in terms of paragraph (a) or cause it to be returned to the person or organization responsible for the transmission of the postal article or telegram, for transmission to the addressee concerned if such postal article or telegram, in the opinion of-

(i) an officer of at least the rank of major-general in the South

African National Defence Force;

(ii) a member of the Agency or the Service holding a post of at least chief director; or

(iii) an officer of at least the rank of assistant-commissioner in the South African Police Service or a member of the said Police Service occupying a post on at least the same level,

may be returned without prejudice to the maintenance of law and order in the Republic or without prejudice to the security of the Republic, as the case may be;

(c) on the instructions of the officer or member who made the application in terms of section 3 (2), dispose of the postal article or telegram that was taken into possession in terms of paragraph (a) in such manner as the maintenance of law and order in the Republic or the security of the Republic requires, if such officer or member, as the case may be, is of the opinion that the postal article or telegram concerned cannot be returned in terms of paragraph (b) without prejudice to the maintenance of law and order in the Republic, or without prejudice to the security of the Republic, as the case may be.

(3) The officer or member who granted the authorization referred to in subsection (1), may authorize such number of members to assist with the execution of the direction as he deems necessary.

(4) A member who executes a direction or assists with the execution of a direction may at any time enter upon any premises in order to install, maintain or remove a monitoring device, or to intercept or take into possession a postal article, or to intercept any communication, or to install, maintain or remove a device by means of which any communication can be intercepted, for the purposes of this Act.

5 Assistance at execution of direction by certain persons or organizations

(1) If a direction referred to in section 2 (2) or a copy thereof is handed to the person or organization who is responsible for the dispatching of a postal article or the transmission of a communication over a telecommunications line, or for the rendering of a postal service or telecommunication service, to a person, body or organization mentioned in that direction by a member who executes that direction or assists with the execution of that direction, the person, body or organization concerned shall as soon as possible-

(a) intercept the postal article or telegram concerned or all postal articles or telegrams to which the direction applies and hand it or them over to a member who is authorized in terms of section 4(1) to execute the direction concerned or to assist with the execution thereof;

(b) make available the necessary facilities and devices and enable the member who is authorized in terms of section 4 (1) to execute a direction

or to assist with the execution of a direction, to effect the necessary connections in order to monitor conversations or communications to which the direction applies.

(2) If a person, body or organization has made a facility, device or telecommunications line available for the purposes mentioned in subsection (1) (b), the remuneration agreed upon by the person or organization and the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force or the Director-General of the Agency or the Service, as the case may be, shall be paid to that person, body or organization.

(3) If an agreement is not reached in terms of subsection (2), a reasonable remuneration shall be determined by the Minister for Posts, Telecommunications and Broadcasting, with the concurrence of the Minister of State Expenditure, in order to compensate the person, body or organization at least for any costs incurred as a result of any action in terms of this Act.

6 Directives regarding applications

The respective Judges-President of the Supreme Court of South Africa may jointly issue directives in which the manner and procedure of applications in terms of section 3 (1) and (4) are uniformly regulated.

7 Secrecy

(1) Any person who is or was concerned in the performance of any function in terms of this Act, shall not disclose any information which he obtained in the performance of such a function except-

(a) to any person who of necessity requires it for the performance of his functions in terms of this Act;

(b) if he is a person who of necessity supplies it in the performance of his functions in terms of this Act;

(c) such information which is required in terms of any law or as evidence in any court of law; or

(d) to any competent authority which requires it for the institution, or an investigation with a view to the institution, of any criminal prosecution.

(2) An employee of a person, body or organization referred to in section 5(1) shall not disclose any information which he obtained in the course of his employment and which is connected with the performance of any function in terms of this Act, whether that employee is involved in the performance of that function or not, except for the purposes mentioned in subsection (1) (a) to (d).

8 Offences and penalties

(1) Any person who contravenes a provision of section 2 (1) or 7 shall be guilty of an offence and liable on conviction-

(a) in the case of a contravention of section 2 (1), to a fine, or to imprisonment for a period not exceeding two years; or

(b) in the case of a contravention of section 7, to a fine, or to imprisonment for a period not exceeding five years.

(2) Notwithstanding anything to the contrary in any other law contained, a magistrate's court shall be competent to impose any penalty provided for in this Act.

9 Repeal of laws, and saving

(1) Section 118A of the Post Office Act, 1958 (Act 44 of 1958), is hereby repealed.

(2) A direction issued under section 118A (1) of the Post Office Act, 1958, and which is still in force at the commencement of this Act, shall be deemed to be issued under section 2 (2) of this Act by the judge referred to in section 3 (1) (a) of this Act and shall remain in force until the period or extended period for which that direction has been issued, lapses.

10 Short title and commencement

This Act shall be called the Interception and Monitoring Prohibition Act, 1992, and shall come into operation on a date fixed by the State President by proclamation in the Gazette.

Annexure C

THE INTERCEPTION AND MONITORING PROHIBITION AMENDMENT BILL, 1999
AS PROPOSED IN DISCUSSION PAPER 78

BILL

To amend the Interception and Monitoring Prohibition Act, 1992, so as to prohibit the provision of telecommunication services which are not capable of being monitored, to make provision for a dual system of consideration of applications, namely for crime and security related applications respectively, to regulate the enabling of monitoring in terms of the Act by persons, bodies or organizations rendering a telecommunication service of conversations and communications, and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:-

Amendment of section 1 of Act 127 of 1992, as amended by section 32 of Act 38 of 1994, section 1 of Act 77 of 1995 and section 13 of Act 34 of 1998

1. Section 1 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended -

(a) by the insertion, after the definition of "Agency" of the following definition:

"call-related information" includes dialling or signalling information that identifies the origin, direction, destination termination, duration and equipment identification of each communication generated or received by a user of any equipment, facility or service of a person, body or organization rendering a telecommunication service, and where applicable the location of such user."

(b) by the substitution for the definition of "judge" of the following definition:

"'judge' means any judge of any provincial or local division of the **[Supreme]** High Court of South Africa, including any judge discharged from active service under section 3 of the Judges' Remuneration and Conditions of Employment Act, 1989 (Act No 88 of 1989), and any retired judge, who is designated by the Minister of Justice to perform the functions of a judge **[within a particular division]** for the purposes of this Act."

(c) by the substitution for the definition of "serious offence" of the following definition:

"'serious offence' means -

(a) any offence mentioned in Schedule I to the Criminal Procedure Act, 1977 (Act No. 51 of 1977), including any conspiracy, incitement or attempt to commit any offence referred to in that Schedule, provided that -

(i) that offence is allegedly being or has allegedly been committed over a lengthy period of time;

(ii) that offence is allegedly being or has allegedly been committed

on an organized, planned or premeditated basis by the person or persons involved therein;

(iii) that offence may allegedly harm the economy or other interests of the Republic; or

(b) any offence referred to in sections 13 (f) and 14 (b) of the Drugs and Drug Trafficking Act, 1992; or

(c) any offence relating to the trafficking in firearms, ammunition and explosives;

(d) any offence relating to the death or serious bodily harm of any person;

(e) any offence relating to organized crime, money-laundering or the proceeds of crime.

(d) by the insertion, after the definition of "telecommunications line", of the following definition:

"telecommunication service" means any telecommunication service as defined in the Telecommunications Act, 1996 (Act No. 103 of 1996), in respect of -

(a) a public switched telecommunication service;

(b) a mobile or a fixed cellular telecommunication service;

(c) a national long distance telecommunication service;

(d) an international telecommunication service; or

(e) any other telecommunication service licensed as such in terms of the Telecommunications Act, 1996.

Amendment of section 2 of Act 127 of 1992, as amended by section 14 of Act 34 of 1998

2. Section 2 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended by the substitution for paragraph (b) of subsection (1) of the following paragraph:

"(b) intentionally monitor any conversation or communication, between two or more other persons without their knowledge or permission, by means of a monitoring device so as to gather confidential information concerning any person, body or organization."

Amendment of section 3 of Act 127 of 1992, as amended by section 32 of Act 38 of 1994, section 4 of Act 18 of 1996, and section 15 of Act 34 of 1998

3. Section 3 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended by -

(a) the substitution for paragraph (a) of subsection 1 of the following paragraph:

"(a) designated by the Minister of Justice **[for the Division]** -

(i) **[from where the postal article or communication referred to in section 2(2)(a) or (b) has been or will probably be dispatched or transmitted or where that postal article or communication will probably be received; or]** in each division to consider only applications in terms of this Act relating to serious offences: Provided that the Minister may designate a judge for more than one division, and

(ii) **[where the proposed monitoring referred to in section 2(2)(c) will be carried out; and]** to consider only applications in terms

of this Act relating to the security of the Republic, and "

(b) the substitution for paragraph (b) of subsection (1) of the following subparagraph:

"(b) if the judge is **[convinced]** satisfied, on the grounds mentioned in a written application that complies with the directives referred to in section 6-

(i) that the offence that has been or is being or probably will be committed, is a serious offence that cannot be properly investigated in **[any other]** another, less intrusive, manner and of which the investigation in terms of this Act is necessary.

(ii) that the security or the interests of the Republic is threatened or that the gathering of information concerning a threat to the security or the interests of the Republic is necessary";

(c) the insertion of the following subsection:

"(7) No communication between a legal representative and his or her client may be intercepted or monitored, except if on reliable information, the judge is satisfied that such a legal representative is involved in, or aiding or abetting a serious offence."

Amendment of section 5 of Act 127 of 1992, as amended by section 32 of Act 38 of 1996, section 4 of Act 18 of 1996 and section 17 of Act * of 1998

4. Section 5 of Act 127 of 1992, is hereby amended by the insertion of a new subsection (4) -

"(4) The remuneration referred to in subsections (2) and (3) shall only be in respect of direct costs incurred in respect of personnel and administration and the lease of telecommunications lines, where applicable, and shall not include the costs of acquiring the facilities and devices referred to section 5A(2)."

Insertion of sections 5A and 5B in Act 127 of 1992

5. The following sections are hereby inserted after section 5 of the Interception and Monitoring Prohibition Act, 1992 -

Prohibition on certain telecommunications services:

5A(1) Notwithstanding the provisions of any other law, no person, body or organization rendering a telecommunication service, may provide any such service which is not capable and does not have the capacity to be monitored.

(2) Any person, body or organization rendering a telecommunication service shall at own cost and within the period specified by the Minister responsible for Communications, in a directive referred to in subsection (6), acquire the necessary facilities and devices to enable the monitoring of conversations and communications, of which the monitoring has been authorized in terms of this Act, from a supplier approved by the Minister responsible for Communications.

(3) The investment, technical, maintenance and operating costs in enabling a

telecommunication service to be capable of being monitored, shall be carried by the person, body or organization rendering such a service.

(4) Duplicate signals of conversations and communications authorized to be monitored in terms of this Act, shall be routed by the relevant person, body or organization rendering a telecommunication service to the relevant central monitoring centre, to be designated by, respectively, the National Commissioner of the South African Police Service, the Chief of the South African National Defence Force, and the Directors-General of the Agency and Service.

(5) The South African Police Service, the South African National Defence Force, the Agency and the Service shall, at State expense, equip and maintain central monitoring centres for the authorized monitoring of conversations or communications: Provided that an agreement on the sharing of any such central monitoring centre shall not be excluded.

(6) The Minister responsible for Communications may issue a directive to any person, body or organization rendering a telecommunication service, to comply with subsection (1) and may, in such direction, specify the security, technical and functional requirements of the facilities and devices to be acquired in terms of subsection (2).

(7) The directives referred to in subsection (6) may include, but are not limited, to specifications on the following -

(a) the capacity needed for interception purposes;

(b) systems to be used;

(c) connectivity with designated central monitoring centres;

(d) the manner of transmission of duplicated signals of conversations and communications to be intercepted, to the designated central monitoring centres referred to in subsection (5); or

(e) the manner of transmission of call-related informationto the central monitoring centres, referred to in section 5B.

(8) The Minister for Posts, Telecommunications and Broadcasting may determine a period, which shall not be less than three months from the date on which a direction in terms of subsection (6) is issued, for compliance with such a direction.

Call-related data

5B(1) Any person who is authorized to apply for a direction referred to in section 2(2), may also apply, in the manner prescribed in this Act for the application for a direction for interception or monitoring, for the provisioning on an ongoing basis of call-related data relating to the conversations or communications mentioned in the direction, and the judge may authorize such provisioning in the same direction.

(2) Any person, body or organization rendering a telecommunication service shall, in respect of all conversations or communications which are monitored in terms of this Act, route the call-related data specified in a direction referred to in subsection (1) and section 2(2), to the relevant designated central monitoring centre.

(3) If, in a specific case, only call-related data is required on an ongoing basis without the actual monitoring of the conversation or communication in question, the judge may direct that the relevant person, body or organization rendering a telecommunication service to whom or which a direction is addressed, provide such call-related data for purposes relating to the functions of the South African Police Service, the South African National Defence Force, the Agency or the Service, whatever is applicable.

(4) The above procedures in respect of the ongoing provisioning of call-related data does not exclude the use of any other power in any other Act, to obtain evidence or

information in respect of a person, body or organization.

(5) Any person, body or organization rendering a telecommunication service, shall provide such information regarding users of such telecommunication service to the South African Police Service, the South African National Defence Force, the Agency or the Service, as may be required by an officer or member referred to in section 3(2)(a), (b) and (c) to fulfil the functions and exercise the powers authorized by law.

(6) The obligation in terms of subsection (5) includes the provision of the name, identity number and address of the person using a specific telecommunications number.

(7) Any person, body or organization rendering a telecommunication service shall -

(a) ensure that proper records regarding identities and addresses are kept in respect of clients to whom a telecommunication service are contracted, whether on a prepaid or contract basis;

(b) require positive identification from a client to whom such a service is contracted.

Amendment of section 6 of Act 127 of 1992

6. Section 6 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended by the insertion of the following subsection:

"(2) The judge referred to in subsection 3(1)(a) may in any case considered by him or her to be sufficiently urgent, dispense with the procedure contemplated in subsections (1) and may deal with the matter in such manner and subject to such conditions as he or she may deem fit, including the grant in any appropriate case of an oral direction followed up by a written application within one week".

Insertion of section 6A in Act 127 of 1992

7. The following section 6A is hereby inserted in the Interception and Monitoring Prohibition Act, 1992, after section 6:

"6A(1) The use of any information obtained through the application of this Act, or any similar Act in another country, as evidence in any prosecution, is subject to any guidelines of the Director of Public Prosecutions or Investigating Director contemplated in the National Prosecuting Authority Act, 1998 (Act No 32 of 1998) concerned, which may include an obligation to obtain the Director of Public Prosecutions or Investigating Director's permission to use the said information as evidence, if so required by the Director of Public Prosecutions or Investigating Director."

(2) The information regarding the commission of any criminal offence, obtained by means of any interception or monitoring in terms of this Act, or any similar Act in another country may be admissible as evidence in criminal proceedings, irrespective of the grounds on which the direction has been granted.

Alternative clause 6A(2)

(2) The information regarding the commission of any criminal offence, obtained by means of any interception or monitoring in terms of this Act, or any similar Act in another country may be admissible as evidence in criminal proceedings.

Amendment of section 8 of Act 127 of 1992

8. Section 8 of the Interception and Monitoring Prohibition Act, 1992, is hereby amended by-

(a) substituting the following subsection for subsection (1):

(1) Any person who contravenes a provision of section 2(1) or 7 shall be guilty of an offence and liable on conviction-

(a) in the case of a contravention of section 2(1), to a fine not exceeding R20000, or to imprisonment for a period not exceeding two years;

(b) in the case of a contravention of section 7, to a fine not exceeding R40000, or to imprisonment for a period not exceeding five years;"

(b) the insertion after subsection (1) of the following subsection:

"(1A) Any person, body or organization rendering a telecommunication service and who or which fails or refuses to comply with -

(a) a direction issued by a judge in terms of section 2(2) or 5B(2);

(b) a directive issued by the Minister for Posts, Telecommunications and Broadcasting in terms of section 5A(6);

(c) the obligation in terms of section 5B(5) to provide information regarding a user of a telecommunication service; or

(d) the obligation in terms of section 5B(7)(a) to keep the records referred to in that section; or

(e) the obligation in terms of section 5B7(b) to require positive identification when contracting a telecommunication service;

shall be guilty of an offence, and liable on conviction, to a fine. Not exceeding R 200 000."

Insertion of section 8A into Act 127 of 1992

9. The Interception and Monitoring Prohibition Act, 1992, is hereby amended by the insertion of the following section:

"8A. If any person, body or organization who or which renders a telecommunication service, after a conviction for failing to comply with a directive issued in terms of section 5A(6), fails to comply with a further directive issued by the Minister for Posts, Telecommunications and Broadcasting to comply with section 5A(1), the said Minister may revoke the licence issued in terms of Chapter V of the Telecommunications Act, 1996, to such person, body or organization to render a telecommunication service.

Transitional arrangements

10. All directions which have been issued by a judge in terms of the Interception and Monitoring Prohibition Act, 1992, when this Act comes into operation, shall remain in force and, unless extended by a judge in terms of section 3, expire on the date determined in the direction.

Substitution of long title of Act 127 of 1992

11. The following long title is hereby substituted for the long title of the Interception and Monitoring Prohibition Act, 1992:

"ACT

To prohibit the interception of certain communications and the monitoring of certain conversations or communications, to prohibit the rendering of certain telecommunication services which are not capable or do not have the capacity to be monitored, to regulate the enabling of such monitoring by telecommunication services; to provide for the interception of postal articles and communications in the case of a serious offence or if the security of the Republic is threatened; and to provide for matters connected therewith."

12. Short title and commencement

7(1) This Act shall be called the Interception and Monitoring Prohibition Amendment Act, 1999.

(2) This Act shall come into operation on a date fixed by the President by Proclamation in the Gazette.

* Judicial Matters Amendment Act, 34 of 1998: To be put into operation by the Department of Justice.

Annexure D

LIST OF RESPONDENTS WHO SUBMITTED WRITTEN COMMENTS ON DISCUSSION PAPER 78

JUDICIARY

1. Judge G Gordon: Office for the Control of Interception and Monitoring of Communications;

LAW SOCIETIES

2. The Law Society of South Africa's Standing Committee on Constitutional Affairs;
3. The Law Society of the Cape of Good Hope's Criminal Law and Procedure Committee;

ADVOCACY

4. Mr Deon van Wyk of the Pretoria Bar;
5. Adv JT Molefe;

UNIVERSITIES

6. Prof Mervyn Dendy: Associate Professor of Law: University of the Witwatersrand;

GOVERNMENT DEPARTMENTS

7. Ms Hellen Naicker of the Department of Public Works;
8. The Director of Public Prosecutions: Cape of Good Hope;
9. Office of the Director Investigating Directorate Organised Crime and Public Safety;
10. Office of the Deputy Minister for Intelligence;
11. Dr PC Jacobs: Chief Manager: Legal Component: Detective Service: SA Police Service;
12. Office of the Deputy Director-General: Operational Services: National Intelligence Agency;
13. Adv M Mnyatheli of the Investigating Directorate: Serious Economic Offences;
14. Office of the Commander: Technical Support Unit: Eastern Cape: SA Police Service;
15. The Joint Communication Security Council and the SA Communication Security Agency;
16. Office of the Director-General: Department of Welfare;
17. Chief Directorate: Legislation and Legal Services: Department of Education;
18. The National Department of Agriculture;

GOVERNMENT BODIES

19. The South African Telecommunications Regulatory Authority;

TELECOMMUNICATION SERVICE PROVIDERS

20. Telkom;
21. Mobile Telephone Networks (Pty) Ltd (MTN);
22. Vodacom;
23. M-Web Connect (Pty) Ltd (M-Web);
24. Globalstar Southern Africa (Pty) Ltd (Globalstar);

MEDIA

25. Reuters Ltd;

BANKING INDUSTRY

26. The Banking Council of South Africa;

SECURITY INDUSTRY

27. Mr Harold Marshall of Marshall International Sales;

OTHER COMPANIES

28. Messrs Paul Sheer, Anton de Wet, Tiaan van Schalkwyk, Francois Wolmerans and Philip Booysen of Obsidian Systems.