SOUTH AFRICAN LAW COMMISSION

DISCUSSION PAPER 78

PROJECT 105

REVIEW OF SECURITY LEGISLATION

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

November 1998

Closing date for comment: 25 January 1999

ISBN: 0-621-28847-0

INTRODUCTION

The South African Law Commission was established by the South African Law Commission Act, 1973 (Act 19 of 1973).

The members of the Commission are -

The Honourable Mr Justice I Mahomed (Chairman)
The Honourable Mr Justice P J J Olivier (Vice-Chairman)
The Honourable Madam Justice Y Mokgoro
Prof R T Nhlapo
Adv J J Gauntlett SC
Ms Z Seedat
Mr P Mojapelo

The Secretary is Mr W Henegan. The Commission's offices are on the 12th floor, Corner Schoeman and Andries Streets, Sanlam Centre, Pretoria. Correspondence should be addressed to:

The Secretary
South African Law Commission
Private Bag X668
PRETORIA
0001

Telephone: (012) 322-6440
Fax: (012) 320-0936
E-mail: pvwyk@salawcom.org.za
Internet site: http://www.law.wits.ac.za/salc/salc.html

The project leader responsible for the project is the Honourable Mr Justice CT Howie.

PREFACE

This Discussion Paper (which reflects information gathered up to the end of June 1998) was prepared to elicit responses and to serve as a basis for the Commission's deliberations, taking into account any responses received. The views, conclusions and recommendations in this paper are accordingly not to be regarded as the Commission's final views. The Discussion Paper is published in full so as to provide persons and bodies wishing to comment or to make suggestions for the reform of this particular branch of the law with sufficient background information to enable them to place focussed submissions before the Commission.

The Commission will assume that respondents agree to the Commission quoting from or referring to comments and attributing comments to respondents, unless representations are marked confidential. Respondents should be aware that the Commission may in any event be required to release information contained in representations under the Constitution of the Republic of South Africa, Act 108 of 1996.

Respondents are requested to submit written comments, representations or requests to the Commission by 25 January 1999 at the address appearing on the previous page. The researcher will endeavour to assist you with particular difficulties you may have. Comment already forwarded to the Commission should not be repeated; in such event respondents should merely indicate that they abide by their previous comment, if this is the position.

The researcher allocated to this project, who may be contacted for further information, is Mr PA van Wyk. The project leader responsible for the project is Mr Justice CT Howie.

INDEX **PAGE NO**

SUMMARY OF RECOMMENDATIONS AND SPECIFIC REQUESTS FOR COMMENT

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

In general, the Interception and Monitoring Prohibition Act, 1992, compares favourably with the legislation of the said countries.

The project committee makes the following general recommendations in this Discussion Paper, namely-

- that the provisions of the Interception and Monitoring Prohibition Act, 1992 be augmented by new provisions-
  - placing an obligation on telecommunication service providers to ensure interceptability/monitoring all communications;
  - 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).

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

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

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;

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 notes 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 does not, however, have definite views on the proviso regarding the requirement of the offence being committed over a lengthy period of time. The committee would appreciate receiving particular comment on this aspect.);

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 invites 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.);

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;

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 is 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 requests specific comment on this issue.);

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 is 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 is suggested empowering the Minister of Justice to designate a judge for more than one division dealing with the serious crime applications. The project committee favours the appointment of a panel of judges.);

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 considers that the required standard should be that of the judge being "satisfied" and not being "convinced". The project committee is of the view that the standard of being "satisfied" will be interpreted as meaning being satisfied on a balance of probabilities.);

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;

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. 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 is 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, furthermore, 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.);

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;

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;

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;

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;

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;

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 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);

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;

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;

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;

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;

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;

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 considers 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.);

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 is 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 is 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, for example along the lines of the United States and Canadian legislation;

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 considers 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.);

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 is 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 notes that 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 notes 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 is of the view that the application of this clause should be confined to serious offences only. The project committee considers that there are two options in regard of the proposed clause: The first option would be 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 is to delete the words "irrespective of the grounds on which the direction has been granted".)

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 notes 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 is 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 is 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 considers 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.);

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.

10.7 The project committee further requests particular comment on the following issues:

- The project committee considers 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 is 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 is defined as one which “renders it primarily useful for the purpose of the surreptitious interception of wire or oral communications”. The committee notes 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. The project committee therefore requests 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?

- The project committee considers 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. (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 considers that this is already implied by the present Act, but that it should be re-formulated to make it more clear.**
- 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 requests particular comment on the question of whether the Bill should set out the procedures to be followed under the Act in more detail.**

BIBLIOGRAPHY

LIST OF CASES

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

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

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

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

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

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

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.

---

[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.

- The protection of classified information in the possession of the State.
- 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. Background

1.9 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 for Human Rights and specifically jurisprudence of the Court regarding interception and monitoring.

1.10. 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.

1.11 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:[3]

> "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,

---

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

- 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 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."

1.12 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.[4] 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

---

[4] 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.

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 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.

1.13 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.[5] 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 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

---

5 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*.

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.

1.14 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".

1.15 This provision of the European Convention on Human Rights is 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 ...."

1.16 The following observation was made in the *Naidoo* case regarding the constitutionality of the Interception and Monitoring Act, 1992:[6]

> "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...."

1.17 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".

1.18 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 Constitution of the United States of America.[7]

1.19 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

---

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

7 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."

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[8] by means of a monitoring device so as to gather confidential[9] 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

---

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

9 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."

concerning a threat to the security of the Republic is necessary.

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

"(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,[10] 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:[11]

> "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

---

10 Supra, p. 214.

11 P. 214.

> 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 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.[12]

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 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[13] 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

---

12 *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."

13 Supra, p. 603 (a-d).

> 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.

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*[14] 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

---

[14] (1997) 3 B HRC 3 (European Court for Human Rights).

principle has been accepted in the case of businesses.[15] 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[16] 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 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.[17] 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

---

15 Supra, 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."

16 *Supra* p. 210, 211.

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

devices is regulated in France by decree.[18] 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 is suggested 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.

---

18 *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.[19]

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

---

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

function to ensure compliance to the recommendations of the 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

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.[20]

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

---

[20] 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.

their employees beforehand that it will be done. Any person may record his own communications without the permission or knowledge of the other party.

4.6 Traffic data (call related data) 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[21] 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*

---

[21] Which serves at present before Parliament and which is expected to be approved shortly.

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 responsible, are the administrative and personnel costs relating to a specific monitoring or request for call related data. 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.[22]

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.

---

[22] Deutscher Bundestag Drucksache 13/8651 01.10.97.

6.5 All the service providers in the telecommunications market have been privatised since 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 data 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 data 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[23]

7.1 The Interception of Communications Act of 1985 came into force on 10 April 1986.[24] 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.[25] 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

---

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

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

25 Section 10(1) of the 1985 Act.

detection of interference with wireless telegraphy.

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[26] 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.[27] 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.[28]

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

---

[26] Section 2(2) of the Act.

[27] Sections 2(1) and 3 of the Act.

[28] Sections 4 and 5 of the Act.

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.[29]

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.[30]

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.[31]

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

---

29 Section 7 of and Schedule 1 to the Act.

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

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

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.[32]

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.

---

[32] Section 8 of Act.

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.[33] 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,

---

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

as no right of privacy exists in such circumstances. FISA does not regulate the use 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."[34]

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,

---

[34] Carr *supra* p. 9-8.

offences relating to the enforcement of the Atomic Energy Act, 1954, or relating to espionage, sabotage, treason or riots;

- ♦ 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.[35]

---

[35] Section 2515 Title III.

8.16 The Communications Assistance for Law Enforcement Act (CALEA) was adopted, inter alia, to regulate the obligations of telecommunications service providers.[36] 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 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.[37]

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

---

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

37 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.

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 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.[38] 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

---

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

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 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.[39] 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.[40]

---

39 Denning, *supra* p. 28.

40 *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.[41] 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.[42] 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

---

41 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.

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

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 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-
> (b) 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.[43] 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

---

[43] 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.

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 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.)

I. 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.[44] 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

---

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

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.[45]

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

---

[45] 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.

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-
> (a) include such provisions as the court considers necessary for the purposes of the order; and
> (b) 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:[46]

> 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

---

46 *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.

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 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*[47] the Canadian Court the court noted that a reasonable

---

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

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 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.[48] 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

---

[48] At p 131.

adapted from their plan for the classification of crimes.[49]

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 Fegan* makes it clear what private communications are.[50] 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

---

[49] 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 ...

[50] *Tremeear's Criminal Code* at p 295.

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 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.[51] Subsection (2) provides that subsection (1) does not apply, to-

(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;

---

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

(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.[52] 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.[53] The Canadian Law Reform Commission explained that the cases of *R v Duarte* and *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

---

52 *Report Recodifying Criminal Procedure* at p 125.

53 *Report Recodifying Criminal Procedure* at p 124.

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,[54] 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

---

[54] 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[55] 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

---

[55] 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.

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.

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.[56]

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

---

[56] 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.

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

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.[57] 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[58] 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.[59] The oath concerned may be administered by telephone or other means of telecommunication.[60] 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.[61]

10.19 Where the judge to whom an application is made is satisfied that the circumstances

---

57 Section 184.3 (1) of the Criminal Code.

58 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.

59 Section 184.3(3) of the Criminal Code.

60 Section 184.3(4) of the Criminal Code.

61 Section 184.3(5).

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 or other means of telecommunication for a period of up to thirty-six hours.[62] 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.[63] 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,[64] 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[65] 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-

---

62 Section 184.3(6).

63 Section 184.3(7)(a).

64 Section 184.3(7)(b).

65 Section 184.4.

(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 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:[66]

---

66 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-

(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

---

(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;
(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.

> 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.[67]

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 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.[68] The Code further provides in section 186(2) that no authorization may be given to intercept a private communication at the office or

---

67 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.

68 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.

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, and 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.[69] 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

---

[69] Section 186.(5).

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 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.[70] 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.[71] 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

---

70 Section 186.(5).

71 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*[72] 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

---

72 (1983) 36 CR (3d) 105.

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.[73]

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

---

[73] Section 188.(6).

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, wilfully

(a) 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.[74] 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 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

---

74 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.

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.[75] 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.[76] 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 were a judgment rendered against the accused in that court in civil proceedings.[77] 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

---

75 Section 194.(1).

76 Section 194.(2).

77 Section 194.(3).

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 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.[78] 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.[79] The Criminal Code provides,

---

78 Section 196.(2).

79 Section 196.(3).

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 the judge to whom each application was made.[80]

---

80 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

10.1 In general, the Interception and Monitoring Prohibition Act, 1992 (Act 127 of 1992), compares favourably with the legislation of the countries discussed above.

10.2 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.

10.3 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.

10.4 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.

10.5 The project committee makes the following general recommendations in this Discussion Paper, namely-

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

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

10.5.1.2 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).

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

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

10.6.2 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;

10.6.3 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 notes 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 does not, however, have definite views on the proviso regarding the requirement of the offence being committed over a lengthy period of time. The committee would appreciate receiving particular comment on this aspect.);

10.6.4 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 invites 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.);

10.6.5 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;

10.6.6 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 is 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 requests specific comment on this issue.);

10.6.7 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 is 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 is suggested empowering the Minister of Justice to designate a judge for more than one division dealing with the serious crime applications. The project committee favours the appointment of a panel of judges.);

10.6.8 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 considers that the required standard should be that of the judge being "satisfied" and not being "convinced". The project committee is of the view that the standard of being "satisfied" will be interpreted as meaning being satisfied on a balance of probabilities.);

10.6.9 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;

10.6.10 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;

10.6.11 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 is 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.);

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

10.6.13 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;

10.6.14 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;

10.6.15 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;

10.6.16 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;

10.6.17 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);

10.6.18 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;

10.6.19 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;

10.6.20 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;

10.6.21 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;

10.6.22 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;

10.6.23 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 considers 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.);

10.6.24 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 is 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 is 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;

10.6.25 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 considers 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.);

10.6.26 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 is 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 notes that 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 notes 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 is of the view that the application of this clause should be confined to serious offences only. The project committee considers that there are two options in regard of the proposed clause: The first option would be 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 is to delete the words “irrespective of the grounds on which the direction

has been granted".)

10.6.27 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 notes 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 is 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 is 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 considers 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 .)

10.6.28 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.

10.7 The project committee further requests particular comment on the following issues:

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

The project committee considers 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 is 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 notes 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, we 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.

10.7.2 **The project committee therefore requests 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?**

10.8 Third party surveillance:

10.8.1 The project committee considers 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. (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 considers that this is already implied by the present Act, but that it should be re-formulated to make it more clear.**

10.9 Should the Act be more prescriptive?

10.9.1 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 requests particular comment on the question of whether the Bill should set out the procedures to be followed under the Act in more detail.**

The Minister of Justice is responsible for the administration of the Interception and Monitoring Prohibition Act, 1992.

A draft Bill, in which the above proposals are addressed, is attached as Annexure “A”.

ANNEXURE "A"

REPUBLIC OF SOUTH AFRICA

INTERCEPTION AND MONITORING PROHIBITION AMENDMENT BILL, 1999

(MINISTER OF JUSTICE)

REPUBLIEK VAN SUID-AFRIKA

WYSIGINGSWETSONTWERP OP DIE VERBOD OP ONDERSKEPPING EN MEELUISTERING, 1999

(MINISTER VAN JUSTISIE)

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, 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 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 "

(c) 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 data to 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 guide-lines 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.