Law Reform Commission of Canada
Commission de réforme du droit du Canada

CRIMINAL LAW

electronic surveillance

Working Paper 47

Canada

Reports and Working Papers of the Law Reform Commission of Canada

Reports to Parliament

1. *Evidence* (December 19, 1975)
2. *Guidelines — Dispositions and Sentences in the Criminal Process** (February 6, 1976)
3. *Our Criminal Law* (March 25, 1976)
4. *Expropriation** (April 8, 1976)
5. *Mental Disorder in the Criminal Process** (April 13, 1976)
6. *Family Law** (May 4, 1976)
7. *Sunday Observance** (May 19, 1976)
8. *The Exigibility to Attachment of Remuneration Payable by the Crown in Right of Canada** (December 19, 1977)
9. *Criminal Procedure — Part I: Miscellaneous Amendments** (February 23, 1978)
10. *Sexual Offences** (November 29, 1978)
11. *The Cheque: Some Modernization** (March 8, 1979)
12. *Theft and Fraud** (March 16, 1979)
13. *Advisory and Investigatory Commissions** (April 8, 1980)
14. *Judicial Review and the Federal Court** (April 25, 1980)
15. *Criteria for the Determination of Death* (April 8, 1981)
16. *The Jury* (July 28, 1982)
17. *Contempt of Court** (August 18, 1982)
18. *Obtaining Reasons before Applying for Judicial Scrutiny — Immigration Appeal Board* (December 16, 1982)
19. *Writs of Assistance and Telewarrants* (July 22, 1983)
20. *Euthanasia, Aiding Suicide and Cessation of Treatment* (October 11, 1983)
21. *Investigative Tests: Alcohol, Drugs and Driving Offences* (November 10, 1983)
22. *Disclosure by the Prosecution* (June 15, 1984)
23. *Questioning Suspects* (November 19, 1984)
24. *Search and Seizure* (March 22, 1985)
25. *Obtaining Forensic Evidence* (June 12, 1985)
26. *Independent Administrative Agencies: A Framework for Decision Making* (October 23, 1985)

Working Papers

1. *The Family Court** (1974)
2. *The Meaning of Guilt: Strict Liability** (1974)
3. *The Principles of Sentencing and Dispositions** (1974)
4. *Discovery** (1974)
5. *Restitution and Compensation** (1974)
6. *Fines** (1974)
7. *Diversion** (1975)
8. *Family Property** (1975)
9. *Expropriation** (1975)
10. *Limits of Criminal Law: Obscenity: A Test Case* (1975)
11. *Imprisonment and Release** (1975)
12. *Maintenance on Divorce** (1975)
13. *Divorce** (1975)
14. *The Criminal Process and Mental Disorder** (1975)
15. *Criminal Procedure: Control of the Process** (1975)
16. *Criminal Responsibility for Group Action** (1976)
17. *Commissions of Inquiry: A New Act** (1977)
18. *Federal Court: Judicial Review** (1977)
19. *Theft and Fraud: Offences* (1977)
20. *Contempt of Court: Offences against the Administration of Justice* (1977)
21. *Payment by Credit Transfer* (1978)
22. *Sexual Offences** (1978)
23. *Criteria for the Determination of Death** (1979)
24. *Sterilization: Implications for Mentally Retarded and Mentally Ill Persons* (1979)
25. *Independent Administrative Agencies* (1980)
26. *Medical Treatment and Criminal Law* (1980)
27. *The Jury in Criminal Trials** (1980)
28. *Euthanasia, Aiding Suicide and Cessation of Treatment* (1982)
29. *The General Part: Liability and Defences* (1982)
30. *Police Powers: Search and Seizure in Criminal Law Enforcement** (1983)
31. *Damage to Property: Vandalism* (1984)
32. *Questioning Suspects* (1984)
33. *Homicide* (1984)
34. *Investigative Tests* (1984)
35. *Defamatory Libel* (1984)
36. *Damage to Property: Arson* (1984)
37. *Extraterritorial Jurisdiction* (1984)
38. *Assault* (1985)
39. *Post-seizure Procedures* (1985)
40. *The Legal Status of the Federal Administration* (1985)
41. *Arrest* (1985)
42. *Bigamy* (1985)
43. *Behaviour Alteration and the Criminal Law* (1985)
44. *Crimes against the Environment* (1985)
45. *Secondary Liability* (1985)
46. *Omissions, Negligence and Endangering* (1985)

The Commission has also published over seventy Study Papers on various aspects of law. If you wish a copy of our catalogue of publications, please write to: Law Reform Commission of Canada, 130 Albert Street, Ottawa, Ontario K1A 0L6, or Suite 310, Place du Canada, Montréal, Québec, H3B 2N2.

* Out of print. Available in many libraries.

ELECTRONIC SURVEILLANCE

Available by mail free of charge from:

Law Reform Commission of Canada
130 Albert St., 7th Floor
Ottawa, Canada
K1A 0L6

or

Suite 310
Place du Canada
Montréal, Québec
H3B 2N2

Catalogue No. J32-1/47-1986
ISBN 0-662-53886-2

Law Reform Commission
of Canada

Working Paper 47

ELECTRONIC SURVEILLANCE

1986

Commission

Mr. Justice Allen M. Linden, President
Mr. Gilles Létourneau, Vice-President*
Ms. Louise Lemelin, Q.C., Commissioner
Mr. Joseph Maingot, Q.C., Commissioner
Mr. John Frecker, Commissioner*

Acting Secretary

Harold J. Levy, LL.B., LL.M.

Co-ordinator, Criminal Procedure

Stanley A. Cohen, B.A., LL.B.

Consultants

Marc Rosenberg, B.A., LL.B.
David Watt, Q.C., B.A., LL.B.

* Was not a member of the Commission when this document was approved.

Notice

This Working Paper presents the views of the Commission at this time. The Commission's final views will be presented later in its Report to the Minister of Justice and Parliament, when the Commission has taken into account comments received in the meantime from the public.

The Commission would be grateful, therefore, if all comments could be sent in writing to:

Secretary
Law Reform Commission of Canada
130 Albert Street
Ottawa, Canada
K1A 0L6

Table of Contents

CHAPTER ONE

Historical Perspective

I. The Common Law Position

The common law has not recognized the privacy of the individual as a discreet legal interest to be afforded specific legal protection. Neither before the advent of modern electronic technology, not thereafter, with the consequent proliferation of surveillance devices, has such a distinct interest in the protection of privacy emerged. Although a number of civil remedies[1] and criminal prosecutions[2] may incidentally afford some protection of the privacy interest, these have as their primary focus other legally protected interests[3] and were considered inadequate in several respects. First, they fail to afford relief to the essence of an invasion of privacy, namely the invasion of one's thoughts, emotions and sensitivities. Instead, they insisted upon a "precondition of proving actual harm beyond insult or hurt" which rendered "most of the old common law torts irrelevant to protecting the intimate interests that may be at stake in defence of individual privacy."[4] Secondly, the criminal law remedies, prosecution for breaches of the *Criminal Code*, were equally inadequate to the task. Their focus, as well, was not upon privacy interests, and any recognition thereby given or remedy thereby afforded, but was primarily directed towards other criminally protected interests.[5] Thirdly, both civil and criminal remedies were anachronistic in view of modern technological advances which permit trespassory invasion without the commission of a trespass and, *a fortiori*, a criminal offence, in conventional terms.[6]

1. For example, trespass, nuisance and negligence actions in relation to the person, chattels or land of the plaintiff.
2. See, for example, *R.* v. *Chapman and Grange*, [1973] 2 O.R. 290, 11 C.C.C. (2d) 84 (C.A.). D's conduct may also engage the prohibitions of paragraph 381(1)(*c*) or (*f*) of the *Code*.
3. For example, the right to enjoyment of one's land enforced by actions in trespass or nuisance.
4. Law Reform Commission of Australia, *Privacy and Intrusions*, [Discussion Paper No. 13] (June, 1980), pp. 24-5.
5. For example, the integrity of contractual and trading relations in Part VIII of the *Criminal Code*, R.S.C. 1970, c. C-34, or the rights of property in Parts VII and IX.
6. Canadian Committee on Corrections, *Report of the Canadian Committee on Corrections, Toward Unity: Criminal Justice and Corrections*, Roger Ouimet, Chairman (Ottawa: Information Canada, 1969), p. 81 (hereinafter cited as the Ouimet Report).

Finally, the principal concern of the common law of evidence is with relevance rather than the manner in which the evidence is obtained. That which is relevant is legally admissible irrespective of the manner in which it has been obtained,[7] provided, of course, it does not contravene any of the exclusionary canons of the law of evidence. The discretion to exclude evidence, otherwise admissible, remains quite limited.[8] Evidence obtained in consequence of invasions of privacy, as for example by the surreptitious recording of telephonic communications, is admissible at common law. This is so notwithstanding the unlawfulness of the conduct used to obtain the evidence, provided it is relevant and properly authenticated.[9]

II. The Ouimet Committee

In its 1969 report, the Ouimet Committee[10] considered that the "interest" which required protection by federal legislation was the privacy of conversations taking place under such circumstances as to justify a reasonable belief on the part of *both* parties that such conversations were not subject to acquisition by others through the use of electronic, mechanical or other devices.[11] As an exception, law enforcement interceptions of private conversations should be permitted, subject to specific conditions and constraints.[12] The Committee would exempt from the scheme of legislative control participant monitoring (consent recording), listening in on extensions and acquiring the contents of conversations taking place in circumstances denuded of any justifiable expectation of privacy.[13] The Committee favoured a system of judicial control of wiretapping and electronic eavesdropping and outlined a proposed scheme in this regard.[14]

The issue of the admissibility of conversations obtained through wiretapping and electronic surveillance was considered. The Committee, which had recommended against a rigid rule excluding all other illegally obtained evidence in favour of a discretion to exclude such evidence, suggested that a separate rule providing for the inadmissibility of such evidence should govern the admissibility of illegally intercepted conversations in view of the unlikelihood of error or inadvertence accounting for such interceptions.[15]

Shortly stated, the Ouimet Committee concluded that as wiretapping and electronic eavesdropping for criminal purposes ought to be suppressed by criminal legislation, so too should its evidentiary fruits. At the same time, the Committee recognized that

7. *Kuruma* v. *The Queen*, [1955] A.C. 197 (P.C.).
8. *R.* v. *Wray*, [1971] S.C.R. 272, [1970] 4 C.C.C. 1.
9. The principal focus of the earlier cases was upon the adequacy of the proof of such issues.
10. Ouimet Report, *supra*, note 6.
11. *Id.*, pp. 82-3.
12. *Id.*, p. 83.
13. *Id.*, p. 85.
14. *Id.*, p. 86.
15. *Id.*, pp. 87-8.

effective law enforcement required electronic surveillance as an investigative aid or tool. While prepared to create an exception for such purposes, the Committee made it plain that such surveillance should require prior judicial authority and be subject to strict control.[16]

III. Federal Protection of Privacy Legislation

The need for federal legislation to control wiretapping and electronic eavesdropping, as identified in the Ouimet Report, assumed legislative form in the proclamation of the *Protection of Privacy Act*[17] on June 30, 1974.

A. Bill C-176

On April 13, 1973, the Minister of Justice introduced Bill C-176 in the House of Commons. The pervasive quality of warranted electronic surveillance was maintained in Bill C-176 by its adopting the same definition of "offence" as was in Bill C-252, namely:

> "offence" means an offence created by an Act of the Parliament of Canada for which an offender may be prosecuted by indictment and includes any such offence that is alleged or suspected or that there are reasonable grounds to believe may be committed; ....

Also, the proposals maintained a distinction between the principles applicable to the admissibility of primary evidence and those which determined whether derivative evidence would be received. In the former instance, inadmissibility was the rule, admissibility the exception. Concerning derivative evidence, the opposite appeared to be so.[18]

Bill C-176 was openly debated at length. Many proposals for amendment were moved, although most of these were defeated.[19] There are but three amendments which merit further comment.

Upon first reading, Bill C-176 had defined "offence" in section 178.1 of the *Criminal Code* in such a way as to include breaches of any federal statute for which an offender may be prosecuted by indictment[20] as well as any such offence that was

16. It was proposed, for example, that the tapes of the conversations recorded pursuant to the order be returned to the authorizing judge.

17. S.C. 1973-74, c. 50.

18. The derivative evidence was said to be inadmissible not solely because the primary evidence from where it was derived was itself excluded.

19. One proposal, in effect, would have limited warranted electronic surveillance to *Official Secrets Act* (R.S.C. 1970, c. O-3) or national security matters.

20. The effect of paragraph 27(1)(*a*) of the *Interpretation Act*, R.S.C. 1970, c. I-23, is also to include dual procedure or Crown option offences in the definition.

alleged or suspected or that there were reasonable grounds to believe may be committed. The definition of "offence" was amended to include a catalogue of offences viewed as sufficiently serious in themselves, particularly appropriate for the use of electronic surveillance, or reflective of the activities of organized crime. The definition not only listed substantive offences but also conspiracies, attempts, or being an accessory after the fact to such listed offences. The final element of the definition was a somewhat circular inclusion: "organized crime."[21] It was felt that the narrower focus of the amended definition, passed by the House, would have a limitary effect upon the intrusive nature of the investigative technique.

Secondly, the House substituted a new section 178.15 for the emergency authorization provision which had earlier been proposed. The initial proposal had not involved, save in an *ex post facto* manner, any judicial officer, but rather had provided for the issuance of emergency permits by the Attorney General of a province, the Solicitor General of Canada or their respective agents specially designated in writing for such purpose. The amendments passed in the House, required approval by a judge and resulted in the present scheme of emergency authorization.

The final amendment made in the House, relates to the admissibility of primary and derivative evidence. The House added, by subsection 178.16(3), a provision whereby both primary and derivative evidence might be admitted, notwithstanding certain formal or procedural defects in the authorization process. It was apparently felt that the additional sanction of the exclusion of credible and relevant evidence was not warranted in view of the criminal prohibition in subsection 178.11(1) of the *Code*.[22]

The *Protection of Privacy Act* remains, at least in several of its most significant aspects, in substantially the same form today as it did at the time of its proclamation on June 30, 1974. The most extensive amendments[23] made to the original legislation obtained final Commons approval on July 18, 1977, and became effective on October 15, 1977. Some of those amendments touch upon matters in respect of which we recommend changes in the present law, so it becomes necessary here to record some brief observations.

B. Bill C-51

Bill C-51 replaced the definition of "offence" by an amendment which listed a variety of substantive offences,[24] included counselling, procuring, inciting, conspirary, attempt and being an accessory after the fact to such offences, as well as a definition of "organized crime."

21. "And that such pattern is part of the activities of organized crime."

22. See, for example, *House of Commons Debates*, First Session, Twenty-ninth Parliament, 22-23 Elizabeth II, Vol. VIII, November 27, 1973, p. 8203 ff.

23. Bill C-51 received first reading on April 20, 1977.

24. The new offences, not all punishable by imprisonment for five years or more, included the crimes in ss. 88, 111, 112, 127, 132, 133(1), 144, 159(1)(*a*), 185(1), 195(1)(*a*) and 340 of the *Criminal Code*, R.S.C. 1970, c. C-34.

The expansion of the definition of "offence" in section 178.1 was also accompanied by an increase in the length of the authorization and renewal periods from the original thirty to sixty days.[25] The proposed increase was founded essentially upon statistical data which demonstrated the average length of warranted interceptions to be in the vicinity of sixty days.[26]

Bill C-51, also added paragraphs (*e*) and (*e*.1)[27] to subsection 178.12(1) making mandatory disclosure, in the supportive affidavit, of the occupations of all proposed named objects of interception, if known. Further, details of any previously unsuccessful or withdrawn applications in relation to a named object and offence have to be disclosed. The purpose of requiring occupational disclosure was linked to the proposals limiting the right to intercept solicitors' communications.[28] The object of the proposals requiring disclosure of unsuccessful and withdrawn applications was at least to control judge shopping.[29]

Finally, Bill C-51 proposed and enacted significant changes to the evidentiary rules applicable in the event that derivative evidence is tendered for admission. The principal change, premised on expediency in the conduct of criminal trials, removed derivative evidence from the reach of the exclusionary rule and made it *prima facie* admissible, subject to the right of the presiding judicial officer to exclude it if its admission would bring the administration of justice into disrepute.[30] The principles upon which primary evidence fell to be admitted were altered only slightly to make it plain that the mere fact that the evidence was tendered in proceedings for an offence other than one authorized in the judicial warrant did not render the evidence inadmissible.[31]

25. No distinction was drawn between authorizations and renewals in this respect.

26. It is arguable that although the amendment had the potential effect of increasing the period over which privacy was invaded, it did so by virtue of an authorization granted upon a more stringent basis than that for renewals.

27. Paragraph 178.12(1)(*e*.1) was not included in the original Bill.

28. Bill C-51, subsections 178.13(1.1) and (1.2).

29. The "solicitor" amendments are at once too wide and too narrow; the former, *inter alia*, because they are not limited to solicitor-client communications, and the latter because they only relate to the "solicitor" half of the problem. The "judge-shopping" amendment only requires disclosure in the event of an earlier failure or withdrawal: the real problem is to prevent the "favourable judge" from being selected in the first instance.

30. Bill C-51, subsection 178.16(1).

31. Subsection 178.16(4) in Bill C-51 as passed: now subsection 178.16(3.1) of the *Code*. It is doubtful if this provision changed the law, at least in those jurisdictions which followed *R*. v. *Welsh and Iannuzzi (No. 6)* (1977), 15 O.R. (2d) 1, 32 C.C.C. (2d) 363 (Ont. C.A.).

CHAPTER TWO

A Case for Reform

I. Introduction

The legislation which enacted Part IV.1 of the *Criminal Code*[32] was presented by the Minister of Justice as legislation to protect the privacy of individuals. It was to be an offence to intercept private communications, disclose private communications and to possess equipment for the purpose of intercepting private communications. However, a case had been made out for the use of electronic surveillance by the police to combat crime; therefore, ancillary to the offence-creating sections was a scheme for judicial authorization of interceptions.

Since the enactment of the legislation, there has been only a handful of prosecutions for the offences in Part IV.1, of which most, if not all, concerned possession of interception devices. Moreover, in some instances the devices involved have been merely police scanners rather than sophisticated interception equipment. On the other hand, there have since been many thousands of authorized wiretaps. The Supreme Court of Canada, in *Goldman* v. *The Queen*,[33] observed that it may be more realistic to say that the purpose or effect of Part IV.1 has been to regulate the method of breach of any such right.

The case for reform in the area of electronic surveillance can be made on two levels. Broadly speaking, there has been an increasing concern as to whether or not the legislation does, in fact, protect persons' legitimate expectations of privacy. The recent enactment of the *Canadian Charter of Rights and Freedoms*[34] brings this concern into sharper focus. Electronic surveillance is a particularly intrusive form of investigation and should be used only in special circumstances where other less intrusive methods would be ineffective. It is a technique which should be employed with restraint. In our consultations throughout Canada, there was no dissent from the proposal that use of electronic surveillance must be accompanied by restraint; nor was there a consensus as to whether the present statutory scheme was being administered with restraint.

32. This and all references to the *Criminal Code* pertain to R.S.C. 1970, c. C-34, as amended.

33. *Goldman* v. *The Queen*, [1980] 1 S.C.R. 976, p. 994; 51 C.C.C. (2d) 1, p. 15, *per* McIntyre J.

34. *Canadian Charter of Rights and Freedoms*, *Constitution Act, 1982*, as enacted by the *Canada Act 1982* (U.K.), c. 11.

The narrower concern is with the mechanics of the legislation. Part IV.1 of the *Criminal Code* is a technical piece of legislation giving rise to initial problems of interpretation. Thus, while the principles of restraint and respect for privacy are important, it is also important that the powers provided to the police be clearly defined "to facilitate the conduct of criminal investigations ... without unreasonably or arbitrarily interfering with individual rights and freedoms."[35]

As this Working Paper is part of the Police Powers Project, it is appropriate that we also be realistic about the legislation; accordingly our primary concern is to define the limits of lawful breach of the "right" to privacy. Thus, the focus of this Paper is the use by police of this method of investigation, not the offence-creating sections. Such reference to the offences is only incidental to the regime of regulation, and is not properly part of our mandate in this Working Paper.

We do not consider that a total overhaul of the present legislative scheme is necessary. The legislation is very recent and, unlike other areas of police powers, tends to reflect twentieth century values and principles rather than those of the seventeenth, eighteenth or nineteenth century. Thus, implicit in the legislation are the principles of restraint, respect for privacy, definition of the powers of the police and judicial review. Where the legislation has failed to accord with these principles in a manner which can be justified by the balancing of interests, we nevertheless believe such problems can be resolved within the framework of the present legislation.

II. The Constitutional Framework

That electronic surveillance is subject to scrutiny under section 8 of the *Canadian Charter of Rights and Freedoms*,[36] which provides that "[e]veryone has the right to be secure against unreasonable search or seizure," is now placed beyond dispute by reason of the Supreme Court of Canada's decision in *Hunter* v. *Southam Inc.*[37] In this judgment, Chief Justice Dickson adopted an approach to section 8 of the Charter premised on the decision of the United States Supreme Court in *Katz* v. *United States*[38] that section 8, like the Fourth Amendment to the United States Constitution, protects the individual's reasonable expectation of privacy and requires a balance between an individual's privacy and the government's interest in law enforcement.[39]

The adoption of the *Katz* reasonable expectation of privacy test is particularly significant for this study, since *Katz* was in fact a wiretap case where the United States Supreme Court held that electronic eavesdropping was within the Fourth Amendment

35. Government of Canada, *The Criminal Law in Canadian Society* (Ottawa: Government of Canada, 1982), p. 61.

36. *Supra*, note 34.

37. *Hunter* v. *Southam Inc.* (1984), 14 C.C.C. (3d) 97 (S.C.C.).

38. *Katz* v. *United States*, 389 U.S. 347 (1967).

39. *Supra*, note 37, p. 128.

protection against unreasonable search and seizure. In the defining of limits to constitutional protection dependent on an assessment of the impact of the government intrusion, one useful guide "is whether, if the particular form of surveillance practiced by the police is permitted to go unregulated by constitutional restraints, the amount of privacy and freedom remaining to citizens would be diminished to a compass inconsistent with the aims of a free and open society."[40] Electronic surveillance obviously comes within that kind of test.

The other significant aspect of the *Hunter* v. *Southam Inc.* case is the court's policy decision to opt for the requirement of prior authorization such as a warrant, except where a warrantless intrusion can be justified. Further, the court requires that the assessment of the competing interests be on a sliding scale depending on the type of intrusion and the state interest involved. The court adopts the "probable cause" standard under section 8 of the Charter for ordinary law enforcement.

As Chief Justice Dickson stated: "The State's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion."[41] In our view, this may have implications in the electronic surveillance context, particularly as regards the validity of "basket clauses," the definition of "private communication," warrantless installation of optical devices, access to material used on the application and minimization, to name just a few. In the one pre-*Hunter* case where it was held that Charter section 8 did apply to electronic eavesdropping, Ewaschuk J. accepted that "the Canadian legislative scheme would violate U.S. constitutional requirements" but that this was reasonable noting that "Canadian legal tradition has, however, traditionally struck the balance more in favour of society than has American tradition."[42] While Ewaschuk J.'s reading of the pre-Charter mood may be correct, we doubt whether the balance under the Charter is now so weighted in favour of "society" (that is, intrusion). It is to be noted that Chief Justice Dickson identified the privacy interest protected by section 8 not with the individual, but with society, to be balanced against the government interest in law enforcement. As he said earlier in the judgment, the constitutionality of a search or 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."[43]

The enactment of the *Canadian Charter of Rights and Freedoms* requires that the legislation be scrutinized with care and that we be alive to potential arguments that certain provisions could offend section 8.

---

40. A.G. Amsterdam, "Perspectives on the Fourth Amendment" (1974), 58 *Minn. L. Rev.* 349, p. 403.
41. *Supra*, note 37, pp. 114-5.
42. *R.* v. *Rowbotham* (1984), 42 C.R. (3d) 164 (Ont. H.C.J.), p. 170.
43. *Supra*, note 37, p. 106.

III. The Balance between Respect for Privacy and Effective Law Enforcement

As we have seen, Part IV.1 of the *Criminal Code*, when originally enacted, was directed at suppression of unlawful wiretapping and control of official electronic eavesdropping. It was absolutely clear that resort to wiretapping and other forms of electronic eavesdropping investigation was to be exceptional. Since the enactment of Part IV.1, and particularly since the 1977 amendments, there has been concern that electronic eavesdropping has been used with far greater frequency than was originally intended and with far fewer restrictions than were envisaged. This concern takes two forms: review of the statistical data in the annual reports, usually in comparison to the American statistics; and secondly, anecdotal reports — use of wiretaps in circumstances which are perceived as trivial or where other less intrusive investigative measures would have succeeded. Unfortunately, the secrecy provisions of Part IV.1, section 178.14, prevent us from directly applying our own judgment to the problem. In any event, since there is no institutionalized objective review of the investigations, other than the limited statistics in the annual reports, it would be difficult to measure the reality of these concerns. The anecdotal "evidence" is suspect since it is so subjective. What defence counsel perceives as a trivial use of the wiretap power may simply be a failure of proof of the important aspect of the investigation.

There are obviously dangers which attend the use of statistics, but certain observations should be recorded. Notwithstanding that the Canadian legislation is similar to, and is in fact based upon, the American legislation, the relative number of authorizations in Canada is nearly twenty to one.[44] Even if we accept that the American legislation is more restrictive, this seems to be an astonishing difference. Furthermore, while section 178.13 contemplates that the authorizing judge will impose terms and conditions, such are virtually never included in the authorization. On the other hand, without our intending to be unduly critical of the judiciary, "basket clauses" have become increasingly wider and almost universal in authorizations.

44. This comparison is based on the 1981 statistics compiled pursuant to section 178.22 of the *Criminal Code* for Canada and by the Administrative Office of the United States Courts for the United States. The figure for Canada is 1,059 and for the United States 589. It should be pointed out that this pattern has remained consistent. Thus, see for example, Louise Savage, "An Analysis of the Federal and Provincial Annual Reports relating to the Use of Court Authorized Electronic Surveillance by Law Enforcement Officials in Canada" (unpublished study prepared for the Law Reform Commission of Canada, 1979), where the figures are set out as follows:

	U.S.	*Canada*
1975	701	1,123
1976	686	1,218
1977	626	1,304

This is despite the fact that, as a result of the 1977 amendments, the maximum length of authorizations was increased from thirty days to sixty days, whereas in the United States the maximum period has remained at thirty days. It should be noted that there were "relatively" fewer renewal applications in Canada (205) while extensions were granted 208 times in the United States.

In our view, the substantial reason for difference in the relative use of the technique between Canada and the United States is that in Canada it is much more cost-effective. It has become clear from consultations with law enforcement authorities in the United States and Canada that wiretapping is an extremely costly and time-consuming business in the United States, as the result of monitoring devices and additional paperwork. There may, of course, be other reasons such as greater disclosure requirements causing the authorities to forego projects which would expose the identities of informants, centralized control over the applications, at least in the federal system, which tends to reduce the number of applications which go forward, and the fact that some states actually prohibit wiretapping.

The obvious implication of the foregoing discussion is that there is a great need for openness in the process. Accordingly, we have approached many of the provisions from the standpoint of requiring justification for secrecy and confidentiality. Needless to say, our consultations with police and prosecutors have been very helpful in identifying legitimate law enforcement concerns and in balancing those concerns with the public's undoubted right to know how the scheme is functioning to the maximum extent which is compatible with such law enforcement objectives.

A review of the case-law surrounding Part IV.1 of the *Criminal Code* has helped to focus on areas of particular concern, areas where Part IV.1 has been difficult to apply, either because of a lack of clarity or direction in the legislation itself, or because the legislation is so different from other Anglo-Canadian legislation that police, lawyers and the judiciary have had difficulty interpreting and applying the provisions.

As a result of the consultation, other problems were brought to our attention, such as the interpretation and application of the legislation which, while never litigated, were sources of concern. We attempt to address those problems as well as we can in our discussions and recommendations.

IV. The Role of the Judiciary

Serious difficulties with the interpretation and application of Part IV.I of the *Criminal Code* were perhaps to be expected, considering that the legislation is based on an American model. The legislation adopts exclusion of evidence as the fundamental sanction. This is not a regime with which Canadian courts are familiar. On the contrary, the general rule in the Canadian context, as expressed in *R.* v. *Wray*,[45] is that evidence is admissible no matter how obtained. The one exception to this rule relates to the admissibility of confessions, and bears no close analogy to exclusion of improperly obtained wiretap evidence. Moreover, derivative evidence from an improperly obtained confession is not subject to the exclusionary rule. The closest analogy to the wiretap regime is that of the search warrant, but at least prior to enactment of the *Canadian Charter of Rights and Freedoms*, it has been clear that improprieties in the obtaining or execution of a search warrant do not render inadmissible the fruits of the search.

45. *Supra*, note 8.

The situation since the enactment of the Charter may, of course, be different. At this stage, it would be wrong to attempt to foresee how the courts will deal with the exclusion of evidence under subsection 24(2) of the Charter in the case of an illegal search made pursuant to an improperly obtained search warrant. Certainly however, serious improprieties in the execution of a search warrant would likely render the evidence inadmissible.[46] It may well be that in the post-Charter era, the exclusion of evidence in the search warrant context will approach the position envisaged by the original wiretap legislation.

The reluctance of the common law to "police the police" through the mechanism of an exclusionary sanction has carried over into the interpretation and application of Part IV.1 of the *Code*. If the exclusion of evidence is to be an effective sanction, those circumstances in which evidence should be excluded must be identified with as much clarity as possible, as attempted in our recommendations.

The other theme which tends to be apparent is a reticence on the part of the judiciary, at the application stage, to see their role as one of supervising the exercise of police discretion. In view of the secrecy which surrounds the application process for authorization to intercept private communications, direct evidence of judicial reticence is not available. There is, however, circumstantial evidence in the statistics created pursuant to section 178.22 of the *Criminal Code*, and a review of those authorizations which, having been adduced at trials, are a matter of public record.

Again, the traditional role of the Canadian judiciary is not to become involved in the pretrial investigation. The one important exception, that of issuing search warrants, has a long history and, as the Commission's studies in that area have revealed, the degree of judicial control actually exercised is, at best, uneven.[47] Again, accepting Parliament's judgment that judicial control is necessary, it would seem to us that the circumstances in which authorizations should and should *not* be granted must be identified and spelled out, as must the contents of the authorization. In fact, the *Canadian Charter of Rights and Freedoms* would likely compel the conclusion that judicial control is appropriate. The legislation must recognize that it is essentially unfair to expect a judge, who is used to being the impartial arbiter, in effect to accept a supervisory role over the prosecution, without some very clear guidelines as to the limits of his authority. We feel that it is primarily up to Parliament, rather than the judiciary, to strike the balance between a justifiable intrusion and an unwarranted invasion of privacy, although obviously in the particular case the ultimate decision must be for the judge to make.

Although during the course of our consultations we encountered a spectrum of views concerning the degree to which the legislation should set out the criteria for granting the application, including terms or conditions, exclusion of evidence and so on, there was considerable consensus that the necessary flexibility could be accommodated within a statutory framework which would give more direction to the judiciary.

46. *R.* v. *Rao* (1984), 12 C.C.C. (3d) 97 (Ont. C.A.).

47. Law Reform Commission of Canada, *Police Powers — Search and Seizure in Criminal Law Enforcement*, [Working Paper 30] (Ottawa: Minister of Supply and Services Canada, 1983), p. 137 (hereinafter cited as the Search and Seizure Working Paper). Also see K.W. Lidstone, "Magistrates, the Police and Search Warrants," [1984] *Crim. L. Rev.* 449.

CHAPTER THREE

Our Recommendations and Commentary

This chapter of the Paper is structured so as to identify the problems, consider the options and make recommendations. It does not necessarily track the present legislation section by section. Rather, we have attempted to deal with areas of concern which often requires looking at several different sections. However, the present Part IV.1 of the *Criminal Code* must be seen as the background against which the recommendations would operate. Nevertheless, the relevant part of the present Part IV.1 is always referred to, if not quoted in full.

I. Application of Part IV.1 of the *Criminal Code*

A. The Offence

The principle of restraint would generally require that the investigative tool which is one of the most intrusive be resorted to only in the most serious cases or where it is most likely to produce results with a minimum of interference to legitimate privacy interests. *Code* section 178.1 presently defines "offence" by listing numerous offences under the *Criminal Code*, as well as some offences under other federal statutes, and incorporating a blanket provision relating to any other offence under the *Code* for which a maximum sentence of five years or more, or an offence mentioned in section 3 or 20 of the *Small Loans Act* "that there are reasonable and probable grounds to believe is part of a pattern of criminal activity planned and organized by a number of persons acting in concert; ...."[48] The importance of the law enforcement officers' need to use this type of tool was recognized, as members of organized crime and persons involved in very serious lucrative crime will use any equipment and techniques available to them.[49]

In the United States, at the time of adoption of Title III, organized crime was put forward as virtually the *raison d'être* for the legislation.[50]

48. *Criminal Code*, s. 178.1.

49. Canada, House of Commons, *Minutes of Proceedings of the Standing Committee on Justice and Legal Affairs*, June 5, 1972, Issue No. 13, p. 13:7.

50. American Bar Association, project on *Minimum Standards for Criminal Justice, Standards Relating to Electronic Surveillance* (Tentative Draft, June, 1968).

The ideal use of electronic surveillance to combat organized crime, it seems, would be as an intelligence-gathering mechanism. The ideal order, then, would tend to be person-oriented rather than offence-oriented, and would be of indefinite duration. On the other hand, there are serious problems with such a regime which were recognized at the time Part IV.1 was enacted. Perhaps the most obvious problem is that of satisfactorily defining "organized crime." The definition in *Code* section 178.1 is really little more than the definition of a conspiracy. Further, the Commission has rejected intrusions which perform a purely intelligence-gathering function, and has observed that "the general rule must be that intrusions upon these rights can only be justified following the initiation of an offence."[51] We consider this principle to be as applicable in the area of electronic surveillance as in the area of search and seizure. We are not persuaded that it is a principle which can be sacrificed on the basis of combating organized crime. We believe that the concerns as to the serious threat to life and property represented by organized crime and the difficulty of investigating that activity can be effectively met by a regime which is offence-specific and permits the granting of an authorization to investigate a conspiracy to commit such an offence (as does the present legislation).

Further, while some of the debate concerning Part IV.1 of the *Code* centred upon the utility of wiretapping as a means of combating organized crime, wiretapping has clearly not been limited to such activity. Thus, we think it inappropriate to design a wiretap regime premised on identifying offences committed by organized crime. We see no reason why trivial offences should fall within the wiretap regime because they may be committed by organized crime, nor do we see why serious crimes should be excluded because they are not traditionally committed by organized crime. We are also not convinced that the number of applications for a particular offence in the past is any measure of the need to include such an offence in Part IV.1. We accept, of course, that the large number of authorizations for certain offences is a measure of their utility in the investigation. On the other hand, the relatively small number of authorizations for investigating kidnappings or murders does not mean that, where appropriate, it is not vitally important that wiretapping be available to aid in the investigation.

While we see no alternative to listing offences, we think that it is possible, at the very least, to adopt criteria for including an offence in the list. In its *Fourth Report*, the Standing Committee on Justice and Legal Affairs proposed that the offence be a serious crime which threatens life, and individual and group well-being, to such an extent that the protection of privacy must yield to protection against antisocial activities.[52] The standard adopted by the American Bar Association in *Standards for Criminal Justice*[53] is that the offences be serious in themselves or characteristic of group activity. The advantage of the latter criterion is that it contains an element which focuses on the utility of wiretapping as an investigative tool. It seems reasonable that offences which are characteristic of group activity and thus require communication among participants, would likely be susceptible to wiretapping, and that wiretapping would produce

51. Search and Seizure Working Paper, *supra*, note 47, p. 137.

52. Canada, House of Commons, Standing Committee on Justice and Legal Affairs, *Fourth Report*, 1970.

53. American Bar Association, *Standards for Criminal Justice*, 2nd ed. (Boston: Little, Brown and Company, 1980).

significant quantities of evidence. In our view, the American Bar Association standard can be represented at the two extremes by murder as an offence which is serious in itself, and gambling as one characteristic of group activity. We think that both of these offences should properly be subject to wiretapping — murder because of its obvious seriousness, gambling because of the high degree of probability that *properly controlled* electronic surveillance would produce a high quality of evidence involving a minimum interference with legitimate privacy interests in circumstances where the offence would be otherwise difficult to detect. For both types of offences, the regime which we propose would attempt to ensure at the legislative level that there be a reasonable likelihood of useful evidence being obtained and, for the less serious offences, that the degree of intrusion be limited.

It has been argued that the definition of "offence" can be rationalized by simply permitting an authorization in the case of any indictable offence in the same way that a search warrant can be obtained in relation to *any* offence. We are not persuaded that such a rationalization is desirable or that the availability of a search warrant is the appropriate analogy in this regard. While the search of a person's home or office is certainly intrusive, it is qualitatively different from the intrusion contemplated by electronic surveillance. Even the most wide-scale search is an event lasting, at the longest, a day or two. It is directed towards uncovering existing evidence or contraband which there is a substantial likelihood not only exists, but exists in the place sought to be searched. Authorization of a wiretap, however, is predicated on the lack of existing evidence. It is not primarily directed at uncovering contraband or evidence, but is authorized in the expectation that evidence will be produced, not in the form of objects or documents but in the targets revealing their thoughts and ideas through communication. The search warrant analogy is valid only to the extent that it suggests the one parameter, namely that less "serious" offences should be targets of interception only where there is a substantial likelihood of uncovering evidence. The search warrant analogy is otherwise properly put in focus by considering whether a justice would knowingly authorize the daily search of premises for thirty to sixty days, the duration of most authorizations, no matter how serious the offence and how certain the prospect of obtaining evidence or contraband.

There is one other limited area which does not clearly fit into the dual standard, and that is offences which are integral to the wiretap regime itself, namely the offences created in *Criminal Code* sections 178.11 and 178.18. Our search of the annual reports made pursuant to section 178.22, which were available to us, has not turned up any resort to these provisions. On the other hand, inclusion of these offences in section 178.1 makes a statement about the commitment to privacy, since these offences really underlie the basic thrust of the legislation — namely, that unauthorized, nonconsensual wiretapping should be illegal.

Finally, we consider that the group activity criterion must be used with restraint. There should be a high degree of probability, from the nature of the offence, that evidence can only be obtained in this way. Further, offences which are not well defined in the *Code*, the investigation of which may infringe on fundamental values such as freedom of expression, should not be included in the list.

We recommend relatively minor changes to the present list of offences for which an authorization may be obtained. Our major recommendation, the elimination of the organized crime basis, was widely accepted, as most persons consulted agreed that it defied definition or proper application and was a potential source of abuse.

RECOMMENDATIONS

1. That the offences for which an authorization would be available continue to be listed. That the following offences be omitted from the present list in section 178.1: *Criminal Code* ss. 58 (forgery, etc.), 159 (obscene material), 195(1)(*a*) (procuring), 281.1 (advocating genocide), 314 (theft from mail), 331 (threatening letters, etc.), 339 (using mails to defraud); and *Excise Act*: ss. 158 and 163 (unlawful distillation or selling of spirits).

2. That the following *Criminal Code* offences be added to the list: ss. 195(1)(*b*), (*c*), (*d*), (*h*), and (*i*) (procuring, etc.), 305.1 (criminal interest rate),[54] 381.1 (threats to commit offences against internationally protected person).[55]

3. That the organized crime definition for offences be omitted but an authorization be available for investigation of: a conspiracy to commit; attempt to commit; being an accessory after the fact; and counselling, procuring or inciting in relation to any of the listed offences.

B. Private Communications

An essential aspect of the operation of a legislative scheme for the control of electronic surveillance is the decision as to which communications it is intended to protect. The definition of private communication recognizes that there is an inherent value in protecting privacy. While Part IV.1 of the *Code* contemplates (in paragraph 178.16(1)(*b*)) the use of evidence obtained as a result of unlawful interceptions if a

54. Addition of this offence perhaps requires some explanation. Deletion of the "organized crime" definition removes reference to the federal *Small Loans Act* (R.S.C. 1970, c. S-11). The intent of that reference was an attempt to deal with "loansharking," an offence often associated with "true" organized crime and with extortion. This area is now covered by the new *Criminal Code* section 305.1, and like extortion (section 305), it should be a targetable offence. It is an offence where the victim is particularly vulnerable and thus where effective enforcement may depend on the availability of evidence obtainable from the interception of communications.

55. Bill C-18, which was passed by Parliament, proposes in section 22, certain changes to *Code* section 178.1 which, in part, are similar to this recommendation. It does not eliminate any offences other than section 331 and paragraph 195(1)(*a*) (procuring) which however is replaced by a reference to "s. 195(1) (procuring)." As will be seen, we also recommend changes to section 195, but by replacing the reference to paragraph 195(1)(*a*) by a reference to other paragraphs which have the connotation of force and compulsion. Some of the offences in subsection 195(1) are simply not serious enough to warrant their inclusion.

party consents to the admission of the evidence, there is no question that the thrust of the legislation is to control the lawful use of electronic surveillance while criminalizing its unlawful use. " '[P]rivate communication' means any oral communication or any telecommunication made under circumstances in which it is reasonable for the originator thereof to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it; ...."[56]

While it is only those activities in which a person has a reasonable expectation of privacy which require legislative control, the increasing use (real or perceived) of electronic surveillance by state agencies has led to the uncomfortable prospect that it is not unreasonable for persons to suspect that their telephone lines are tapped. If such a trend were to continue, then wiretapping could become uncontrolled, the authorities relying on the societal reasonable apprehension as to the widespread use of wiretapping equipment.[57] This view was expressed by Mr. Justice Brooke, in a recent decision of the Ontario Court of Appeal,[58] who observed that where there was evidence that the respondent knew there was a real danger his telephone communications would be intercepted, it was questionable whether it could properly be said that these communications were made under circumstances in which it was reasonable to expect that they would not be intercepted by any person other than the person whom he intended to receive it.

This displays a certain insensitivity to the purposes behind the enactment of Part IV.1 of the *Code*. Leaving aside "criminals," many innocent persons have nagging fears which could express themselves in similar kinds of utterances to the effect that their telephones are being wiretapped. Writing in 1974, Professor Amsterdam, in another context, focused on the problem of tying regulation of invasions of privacy to the person's subjective reasonable (rather than justifiable) expectation of privacy. He concluded that an "actual, subjective expectation of privacy obviously has no place in ... a theory of what the fourth amendment protects. It can neither add to, nor can its absence detract from, an individual's claim to fourth amendment protection."[59]

The public's legitimate interest in the protection of privacy could be seriously undermined if the definition of "private communication" is not adjusted. A new definition would have to take into account the fact that knowledge as to the existence of wiretapping is becoming more prevalent, while making it clear that a party to a "private" communication still has a "reasonable" expectation of privacy where his only concern centres on the possibility of lawfully authorized interceptions.

Another problem identified in the definition of "private communication" was discussed in the decision of the Supreme Court of Canada in *Goldman* v. *The Queen*.[60] In that case, it was argued that the communications which had been intercepted by

56. *Criminal Code*, s. 178.1.

57. *R.* v. *Carothers*, [1978] 6 W.W.R. 571 (B.C. Co.Ct.).

58. *R.* v. *Samson* (1983), 9 C.C.C. (2d) 194 (Ont. C.A.), p. 204.

59. Amsterdam, *supra*, note 40, p. 384.

60. *Supra*, note 33.

means of a "body pack" (a radio transmitter worn by the person) were not private communications because the police agent as the "originator" knew of the interception. McIntyre J. resolved the issue in a pragmatic way by holding that the "originator" is the person "who makes the remark or series of remarks which the Crown seeks to adduce in evidence" on the theory that:

> [W]here a police officer or police agent participates in a conversation with a suspect knowing that it is being intercepted electronically and hears the suspect make hoped for inculpatory statements of importance to the Crown's case, I am unable to consider the police officer to be the originator of the very statement or statements he was seeking to obtain.[61]

Without in any way minimizing the difficulty of the problem of interpretation dealt with by the court, we do not believe that it is immediately apparent that the policy of the legislation favours the interpretation adopted by the court. To take the *Goldman* case itself, the only difference between Part IV.1 applying or not, was that additional procedural hurdles had to be overcome to admit the tape of the conversation, than would have been necessary had the police agent been available and able to testify as to his personal recollection of the contents of the conversation. The *privacy* interest in the *Goldman* case is highly abstract in such circumstances. The primary issue is not one of electronic surveillance. That is only incidental to the broader question of the use of police agents. The only genuine justification for the application of Part IV.1 to the *Goldman* situation is that of discovery, namely, making the notice provisions of *Code* subsection 178.16(4) applicable. While there is a policy component, it should be one which encourages compliance with the authorization procedure in situations involving true privacy interests, and which is at the same time a rule that can be applied practically. Even the *Goldman* rule suffers on this latter account since it calls for the court to break up a conversation into separate "communications." In our view, Part IV.1 should protect the privacy of conversations, not individual communications. The overriding policy must be one which favours a simple, practical and easily applied rule. The easiest solution is to define "private communication" to include the entire conversation in which either of the parties has an expectation of privacy. The bodypack problem can be dealt with separately with respect to the admissibility and offence-creating sections.

We were, however, concerned that this new definition could pose problems in two areas: prisons and other lock-ups; and, hostage-taking situations. Under the present legislation, where the hostage taking is a public event with the culprits using the telephone to negotiate with the police or to talk to others, it would not seem that a new definition would pose any problems. It would be unreasonable on anyone's part to believe that such communications were not being monitored;[62] yet that belief may stem from a belief that the monitoring was being done by a court-ordered authorization. The issue is this: Do hostage-taking incidents present such a serious and immediate threat to the lives and safety of others that a special exemption should be built into the proposed definition of "private communication"? If so, then the police would be at liberty to

61. *Id.*, p. 995 (S.C.R.), p. 16 (C.C.C.).

62. See *R.* v. *Gamble and Nichols* (1978), 40 C.C.C. (2d) 415 (Alta. S.C. A.D.), p. 424.

intercept communications in such circumstances without a court authorization. In our view, in such public hostage-taking incidents, the privacy interest is extremely attenuated, while the risk of danger to persons is so extreme that the law must be carefully drafted to ensure that, as before, the public hostage taker's communications with the outside are not "private communications." We believe that Recommendation 4 accomplishes that purpose.

The other problem concerns prison communications. As a matter of security, the communications of inmates with the outside world are monitored by the institution staff. One method of legitimating this process is to post signs on the institution telephones to the effect that the conversation is being or may be intercepted.[63] Under the current definition, such interceptions would not be of private communications, would thus be outside the provision of Part IV.1 and, would therefore not be unlawful. Under our proposed definition, the interception would still be of a private communication, since the party outside the prison might reasonably believe there was no interception. Approached in this manner, the problem is solved not by distorting the definition of "private communication" but by making such interceptions lawful, through an amendment to section 178.11.

There is some controversy as to whether Part IV.1 applies to eavesdropping without the use of electronic devices. In *R.* v. *Beckner*,[64] the court held that Part IV.1 did not apply. However, in the earlier decision in *R.* v. *Boutilier and Melnick*,[65] the contrary result was reached. In our view, the conclusion reached in *Beckner* is correct. While the need to regulate all police intrusions into privacy can be argued, at some point there is a *de minimus* quality to the debate. The corner-stone of any privacy regime is what it outlaws as much as what it permits. To require regulation as to the admissibility of overheard conversations implies the outlawing of such conduct, except in specified circumstances. This would require a radical change in the way most people conduct themselves, even in commonplace everyday activities.[66]

A related problem is a highly technical one arising from the inclusion of "telecommunication" in the definition of "private communications." "Telecommunication" is defined in section 28 of the *Interpretation Act* as meaning "... any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system; ...."

The same definition is also used in *Criminal Code* sections 287 (theft of telecommunication service) and 287.1 (possession of device to obtain telecommunication facility or service). That definition is very wide, and questions have been raised as to whether it would cover the interception of communications transmitted to such things as paying devices which are capable of being private communications within the definition.

63. See *R.* v. *Rodney* (1984), 12 C.C.C. (3d) 195 (B.C. S.C.).

64. *R.* v. *Beckner* (1978), 43 C.C.C. (2d) 356 (Ont. C.A.).

65. *R.* v. *Boutilier and Melnick* (1976), 35 C.C.C. (2d) 555 (N.S. S.C.).

66. See *supra*, note 4, p. 44.

However, the definition might also cover the use of devices sometimes referred to as pen registers which do not acquire any conversation, only the numbers dialed from the telephone. The consensus among law enforcement authorities is that these devices are not covered by the legislation and should be available without having to resort to the authorization procedure. In fact, such a device might be used in preparation of the material to obtain an authorization by assisting to track the members of the alleged conspiracy. It is clear that such devices are not covered by the United States legislation, Title III,[67] which refers only to "aural" interception of private communications. Warrantless use of such devices also does not violate the Fourth Amendment on the theory that a person does not have a reasonable expectation of privacy concerning the numbers dialed.[68] It is our view that there is no reasonable basis for inclusion of the pen register and related devices (such as diode devices used to track the number of an incoming call after the caller has hung up) within the Part IV.1 legislative scheme. Part IV.1 is primarily directed at protecting privacy of communications; that is, discourse between persons. These devices do not invade the privacy of the communication. Moreover, the expectation of privacy in telephone numbers called or received is minimal. To clarify the law in this respect, the proper remedy is a slight adjustment of the definition of "electromagnetic, acoustic, mechanical or other device."

RECOMMENDATIONS

4. That "private communications" be defined as follows:

any oral communication or any telecommunication made under circumstances in which it is reasonable for any party to it to expect that it will not be intercepted by any electromagnetic, acoustic, mechanical or other device.

5. That a communication does not cease to be a private communication only by reason of a belief on the part of a party to it that the communication may be the subject of an authorization obtained from a court by a law enforcement agency.

6. That subsection 178.11(2) be amended by the addition of paragraph (*e*) as follows:

a person engaged in monitoring for security purposes of communications of inmates of a prison as defined by the *Prisons and Reformatories Act*, R.S.C. 1970, c. P-21, and a penitentiary as defined by the *Penitentiary Act*, R.S.C. 1970, c. P-6, where the fact that such monitoring may occur is prominently displayed at the place where the communication may occur.

67. *U.S., Omnibus Crime Control and Safe Streets Act of 1968*, Title III, Act of June 19, 1968, Pub. L. No. 90-351 (hereinafter cited as Title III). See also J.G. Carr, *The Law of Electronic Surveillance* (New York: Clark Boardman, 1977), p. 74.

68. *Smith* v. *Maryland*, 442 U.S. 735 (1979). However, see, *People* v. *Sporleder*, 666 P.2d 135 (Colo. 1983).

7. That the definition of "electromagnetic, acoustic, mechanical or other device" be amended as follows:

> **"electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used, or is capable of being used, to intercept a private communication, but does not include a hearing-aid used to correct subnormal hearing of the user to not better than normal hearing, nor a device such as a pen register, touch-tone decoder, diode device or other similar device used to acquire the identity of the telephone number dialed, or of the caller, the time and the date of the telephone call, but which is not capable of intercepting any words or other information.**

C. Optical Devices

Closely allied to the definition of "private communications" just discussed, and hence the application of Part IV.1, is the problem of the use of optical devices.

It seems clear that the present Part IV.1 does not cover optical devices.[69] In its 1980 discussion paper, the Australian Law Reform Commission identified the use of optical devices as a serious privacy problem (in contrast to the position taken in its Report on *Criminal Investigation*[70]). "In the past simple safeguards could normally be taken by people to secure their privacy against unwanted observation by uninvited third parties. Today, those safeguards are inadequate. Advances in technology have not been confined to listening and interception devices."[71]

While we can appreciate the *potential* for serious privacy issues to arise in the area, there is little evidence at present that the use of optical devices has led to serious abuse or problems of unjustifiable intrusion into privacy. To attempt to legislate in a broad manner in this area would involve serious infringements on the rights of property owners. One cannot legitimately prevent the owners of property such as banks, convenience stores, and so forth from installing cameras to protect the premises from illegal conduct. Another use made of such devices is to record illegal transactions between suspects and police agents. Like the use of body packs, this use of optical devices raises only very theoretical privacy issues. Finally, there is the use of devices such as binoculars and telescopes. The United States Supreme Court has considered this issue in relation to the Fourth Amendment protection against unreasonable search and seizure. In *United States* v. *Knotts*,[72] the court, considering the implications of the use of a

69. *R.* v. *Biasi (No. 3)* (1981), 66 C.C.C. (2d) 566 (B.C. S.C.).

70. Law Reform Commission of Australia, *Criminal Investigation*, [Report No. 2] (Canberra: Australian Government Publishing Service, 1975).

71. *Supra*, note 4, pp. 64-5.

72. *United States* v. *Knotts*, 103 S.Ct. 1081 (1983).

beeper which transmitted an electronic signal permitting officers to monitor the location of the suspect's vehicle, observed that "nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.[73]

Without a great deal more research on the types of devices presently in use and their capabilities, we do not believe that it is possible to legislate in this area in a comprehensive way. It is, however, possible to identify one narrow area where the issues are clear and the privacy interest high, that is, the surreptitious entry of private premises by governmental officials to install optical devices. We propose to regulate such conduct in the same manner as surreptitious entry to install listening devices ("room bugs"), and to leave the other questions for further study. We simply do not feel confident in addressing all the competing policy issues which may arise by adopting a broader test such as regulation of devices in every place where a person has a reasonable expectation of privacy.

Moreover, because we intend to regulate surreptitious entry for installation of listening devices, to leave the area of optical devices unregulated would leave a gap which could permit persons, including law enforcement authorities, to do indirectly what the law otherwise prohibits.

In leaving this subject we wish to make clear that we do not in any way minimize the problems created by law enforcement use of optical devices, even with the consent of the property owner. Whether or not this is an appropriate use of resources, we do not feel that it is an area upon which we can make any recommendation, other than to suggest that the entire field of surreptitious optical surveillance requires study.[74]

RECOMMENDATIONS

8. That it be an offence to enter private property without a court order or the consent of the owner or lawful occupier for the purpose of installing an optical device.

9. That an authorization to install an optical device be available by application to a court, but only under the same conditions as an authorization is available for installation, by surreptitious entry, of a listeining device.

10. That "optical device" be defined for the present time as any electronic device or mechanism capable of permitting surreptitious viewing of persons or things.

73. *Id.*, p. 1086. On the other hand, electronic devices such as a beeper cannot be used to obtain information which would not have been open to visual surveillance, such as a private residence (see *United States* v. *Karo*, 104 S.Ct. 3296 (1984)), notwithstanding that the beeper is less intrusive than a full-scale search.

74. See *U.S.* v. *Torres*, 36 Cr.L. 2301 (December 19, 1984) (7th Cir.), p. 2302.

D. Foreign Interceptions

Another problem which exists with the application of Part IV.1 of the *Criminal Code* is that of interceptions made in foreign countries.

Several recent court decisions in British Columbia have raised the problem of regulation of evidence gathered as the result of an interception made in a foreign jurisdiction. This is an evidentiary problem, since it is conceded that Canadian substantive law can have no reach into other countries so as to attempt to regulate conversations taking place wholly in such countries. Opposing decisions of the British Columbia Supreme Court have held, on the one hand, that the foreign interceptions are inadmissible unless proved to have been lawfully intercepted according to the law of the foreign jurisdiction,[75] and on the other hand, that Part IV.1 did not apply to such interceptions, and admissibility was therefore governed by the general law of evidence.[76] A third option would be to require the interception to conform to Canadian standards. It should be pointed out that this could lead to exclusion of evidence from many countries such as Great Britain[77] where wiretapping is authorized by the Home Secretary rather than by a judge. Neither the application of the principles of criminal procedure nor the interest in protection of privacy immediately identifies the optimal option, or the solution. Canadians who choose to conduct business outside Canada must expect to have that business regulated by foreign governments, and perhaps to have their privacy invaded at the whim of that government.

Other relevant principles are respect for international obligation, economy, clarity and fair and efficient administration of justice. In our view, it would be highly impracticable and disrespectful of international obligations to impose the Canadian regime on foreign governments (the third option).

The one argument presented in favour of the third option is that since the accused is being tried in Canadian courts according to Canadian due process, the evidence presented must accord with Canadian standards of admissibility. The argument is analogous to the confession rule. For example, just as Canadian courts would not accept a confession obtained by torture, even assuming that such activities were lawful in the state where the confession was obtained, so too we should not accept that state's rules in other circumstances. When the accused is tried in Canada, the Canadian rules of procedure must be considered the minimum. Inequality of treatment could arise. Two accused tried in Canada may have had their conversations intercepted, one in Canada, one in the foreign state but by the same means. In the one case, the interception not having been in accordance with Part IV.1, the evidence would be inadmissible. In the other case, the interception, having conformed to the foreign state's lower requirements, would be admissible.

75. See: *R.* v. *Bengert (No. 8)* (1979), 15 C.R. (3d) 37 (B.C. S.C.); *R.* v. *Bengert (No. 9)* (1979), 10 B.C.L.R. 199, 15 C.R. (3d) 40 (B.C. S.C.).

76. *R.* v. *Newall (No. 1)* (1982), 67 C.C.C. (2d) 431, 136 D.L.R. (3d) 734 (B.C. S.C.).

77. See *Malone* v. *Commissioner of Police of the Metropolis (No. 2)*, [1979] 2 All E.R. 620; 69 Cr. App. R. 168 (Ch.D.).

We are not convinced that the logic of these arguments is so compelling as to require the adoption of this third option.

The confession analogy does not really provide a principled basis in the wiretap area. In the first place, confessions are excluded unless voluntarily obtained: (a) to ensure their trustworthiness; and (b) to vindicate the principle against self-incrimination.[78] Neither reason applies to wiretap evidence no matter how obtained. Trustworthiness, in particular, turns on the reliability of the interceptors, not the quality of the legislative scheme which gives them the right to intercept. Further, except for the confession rule, the law in Canada prior to the Charter was that evidence, no matter how obtained, was admissible. Evidence has been used in Canadian and other common law courts, which has been obtained in violation of a host of common law and statutory rights and even in violation of the confession rule[79] without any compunction.

The only due process component upon which Canada can legitimately insist in this area is that resort to the foreign interception was not done in bad faith to avoid the Canadian requirements.

On this question, it would be useful to consider the United States experience, much of which has in fact involved admissibility of communications intercepted by Canadian authorities before and after passage of Part IV.1. Those authorities clearly hold that where the interception was not unlawful under Canadian law (even prior to passage of Part IV.1) the evidence is admissible in United States courts outside of Title III.[80] The authorities, however, are not entirely clear as to the effect of an illegal interception (that is, illegal under the laws of Canada). It seems to depend on the perspective from which the court approaches the question. In *United States* v. *Maher*,[81] the court approached the question from the perspective of the principle underlying the domestic exclusionary rule.

In *United States* v. *Phillips*[82] the court took a broader approach from the perspective that international comity was the principle involved, and it excluded evidence obtained from illegal interceptions (that is, illegal under Canadian law).

Either of these approaches can be defended, depending on the choice of the paramount principle. The approach in *Maher* in particular, which requires domestic connivance, seems suited to the Canadian context. A test for admissibility, which has about

78. *Rothman* v. *The Queen* (1981), 59 C.C.C. (2d) 30 (S.C.C.), *per* Lamer J., p. 63.

79. *R.* v. *St. Lawrence* (1949), 93 C.C.C. 376 (Ont. H.C.J.).

80. *United States* v. *Cotroni*, 527 F.2d 708 (1975), (2d Cir.) cert. den. 426 U.S. 906 (1975); *Stowe* v. *Devoy*, 588 F.2d 336 (1978), (2d Cir.) cert. den. 442 U.S. 931 (1978).

81. *United States* v. *Maher*, 645 F.2d 708 (1981), (9th Cir.), pp. 782-3.

82. *United States* v. *Phillips*, 479 F.Supp. 423 (1979) (M.D. F.C.), pp. 437-8.

it an element of shocking the conscience, is reminiscent of subsection 24(2) of the Charter. It is to be noted that, even under the *Phillips* test, it would appear to place the burden on the accused to demonstrate the illegality under the foreign law.[83]

Accordingly, one solution would be to provide that Part IV.1 applies to foreign interceptions only to a very limited extent. Since the interception takes place outside Canada as explained above, the privacy interest is not paramount. Rather, the paramount principle is concern for vindication of the process itself as indicated by Mr. Justice Lamer in *Rothman* v. *The Queen*,[84] who identified this value when considering the admissibility of a confession obtained by a trick.

Similarly, a blatant disregard for the procedure established in Canada to control interception of private communications ought not to be countenanced. In *Rothman*, Lamer J. considered the appropriate method of control as exclusion of evidence where, by reason of the conduct of persons in authority, to admit the evidence would bring the administration of justice into disrepute. Such a test is similar to the exclusionary rule in subsection 24(2) of the *Canadian Charter of Rights and Freedoms*, although Lamer J. adopted a rigorous test requiring that the conduct

> must be so shocking as to justify the judicial branch of the criminal justice system in feeling that, short of disassociating itself from such conduct through rejection of the statement, its reputation and, as a result, that of the whole criminal justice system, would be brought into disrepute.[85]

It seems unlikely that such a rigorous test would apply under subsection 24(2) of the Charter[86] and we have considered leaving the admissibility of evidence obtained by a foreign interception to be determined by resort to subsection 24(2) of the Charter. However, this could lead to an undesirable uncertainty in the law since it is not at all clear whether conduct by officials outside Canada would constitute violations of a person's rights, a necessary pre-condition to invoking section 24(2), under the Charter. Accordingly, we have opted for a clear but narrow rule focusing directly on what we see as the legitimate Canadian interest, namely protection of the integrity of the system.

We have, moreover, opted to put the initial evidential burden of proof on the accused which, when satisfied, activates the Crown's persuasion burden. We recognize that the practicalities of the matter are that, in most cases, this will effectively preclude investigation of the manner in which the foreign interception was conducted, but we can see no viable alternative.

Finally, we believe foreign interceptions should otherwise be integrated into the regime insofar as notice of introduction into evidence is concerned.

---

83. In *Phillips* that was not difficult, since the case arose out of the Royal American Shows investigation, and there was Canadian judicial authority on the very issue.

84. *Supra*, note 78, p. 72.

85. *Id.*, p. 74.

86. See *R.* v. *Simmons* (1984), 11 C.C.C. (3d) 193 (Ont. C.A.).

RECOMMENDATIONS

11. That primary and derivative evidence obtained from an interception made outside Canada, no matter where the private communication originated, be admissible in evidence whether or not the interception was lawfully made, provided that the interception was not made in the foreign jurisdiction in violation of the laws of the jurisdiction with the connivance of Canadian authorities.

12. That the court before which evidence from a foreign interception is tendered shall conduct an inquiry into the admissibility of that evidence only where the person against whom the evidence is sought to be admitted leads some evidence from which the court could find that the interception was made in violation of the laws of the foreign jurisdiction with the connivance of Canadian authorities.

13. That the notice provisions in present *Code* subsection 178.16(4) apply to evidence obtained from foreign interceptions.

E. Participant Monitoring: Consent Interceptions

Another issue is the question of consent interceptions, made without judicial authorization because a party to the "private" communication agrees to the interception.

Paragraph 178.11(2)(*a*) exempts consent interceptions from the scope of the legislation. This embraces two situations: (1) where one of the participants to the conversation, with or without the knowledge of the other(s), himself tape-records the communication; and (2) a third party with the consent of one of the participants intercepts and records the communication. In view of the *Goldman* v. *The Queen*[87] formulation of "private communications," both these situations embrace private communications at least where the evidence is offered against the nonconsenting party, but in both situations the recording and interception are lawfully made, and evidence so obtained is admissible in evidence *per* paragraph 178.16(1)(*a*). It is the scheme of the legislation that no prior judicial authorization is required.

The Supreme Court of Canada, in *Goldman* v. *The Queen*, indicated that a consent under paragraph 178.11(2)(*a*) is valid and effective "if it is the conscious act of the consentor doing what he intends to do for reasons which he considers sufficient." The consent must be "one he intended to give and if he gives it as a result of his own decision and not under external coercion the fact that his motives for so doing are selfish and even reprehensible by certain standards will not vitiate it." Further, the consent must not be procured by intimidating conduct, force or threats of force by the police, but coercion "does not arise merely because the consent is given because of promised or expected leniency or immunity from prosecution."[88]

87. *Supra*, note 33.

88. *Id.*, p. 1005-6 (S.C.R.), p. 24 (C.C.C.).

This formulation was subjected to some criticism in Working Paper 30, at least at it might apply to search and seizure.[89] We do not think, however, that such a criticism is as valid in the area of consent interceptions. Unlike a "consent" search, a consent interception not only usually involves passive consent but also the active participation of the party.

The most common usage of consent interceptions in the law enforcement context is the recording of a conversation between the suspect and a police agent or an undercover police officer. However, consent recording takes place in many other contexts. Businessmen, for example, may routinely record their own telephone calls or their own meetings. Such a practice is not generally perceived to be illegal.

Concerns have been expressed to the Commission about the desirability of continuing the current system whereby consent interceptions are outside federal control. It may be that even in official use, such interceptions are far more frequent and persuasive than the court-authorized procedure.[90] The concerns have been expressed on two levels, (1) privacy and (2) evidentiary. The privacy concern focuses on the fact that widespread consent recording can, in the long run, compromise the free flow of ideas and affect free speech in an undesirable way. If persons may come to believe that their conversations are being recorded, they will be less candid for fear that their words may come back to haunt them.

The evidentiary concern focuses on the possibility of manipulation by the party who knows of the interception. The knowing party can direct the conversation not only to draw out the suspect and make him incriminate himself, but at the same time may shield his own involvement and produce self-serving evidence. Further, the simple introduction of the tape recording can be misleading to the trier of fact unaware of the effect of the psychology of the situation.

Proposals offered for reform of the law in this area are: first, to continue to provide that consent interception be lawful but not to permit the recording to be introduced into evidence; and second, to bring consent interceptions into line with the rest of the legislative scheme and to require prior judicial approval — the interception, even with consent, would be otherwise unlawful, and the evidence would be subject to exclusion in the same way as other evidence which is the product of the unlawful interception.

We believe that neither proposal is acceptable, and that the law must be maintained essentially as it is now. We have been influenced in this respect by the Australian Law Reform Commission. Although the Commission had, in an earlier paper, suggested adopting a warrant requirement, in its 1983 report on *Privacy*[91] the Commission rejected

89. Search and Seizure Working Paper, *supra*, note 47, pp. 162-3.

90. J.G. Carr, "Electronic Surveillance by Consent under State Law" (November, 1984), 11 *Search and Seizure Law Report* 77.

91. Law Reform Commission of Australia, *Privacy*, [Report No. 22] (Canberra: Australian Government Publishing Service, 1983) (2 volumes).

this view. The reasons given are cogent and equally applicable in the Canadian context (if not more so, considering the ten-year history of legalized consent interceptions). The majority of the Commission stated as follows:

> 1131. *Dangers of Regulating Participant Monitoring.* There are a number of dangers with proposals that participant monitoring, generally, be prohibited. Tape recording of sounds and conversations is now a common practice in purely domestic and friendly circumstances. Tape recordings can be taken of family events, without someone there being aware that it is happening. It can be done at parties for fun. This conduct should not bear the full weight of the criminal law. Accidental recording without the consent of some parties might also occur. The innocent recorder of social events might be placed at a risk completely disproportionate to the undesirability of what he may have done.
>
> 1132. *Fundamental Problem Unresolved.* A person speaking to another does so at his own risk. Whatever he says can be recalled, correctly or incorrectly, by the other parties to the conversation and can be reported, correctly or incorrectly, as they see fit. A person speaking to another must take the risk, ordinarily inherent in so doing, that his hearer will make public what he has heard. There are many ways of recording conversations. Notes written immediately after the conversation has finished is one way. Shorthand notes, or longhand notes, taken during the conversation are others. A listening device simply replaces other techniques of recording that the party to the conversation might use. The fundamental difficulty — the fact that the conversation can be recorded or recalled in circumstances and for purposes outside one party's control — still remains. To regulate the use of some forms of recording does not remove that difficulty.[92]

The first proposal, that is, prohibiting admission of evidence, seems undesirable. Expert evidence, as to the distortion of the nature of the conversation in favour of the knowledgeable participant, can well be called at the trial, just as linguistic evidence has lately been adduced in several trials in an effort to diminish the weight which the trier of fact should attach to a confession.[93] We think it would be wrong, however, as a general rule to exclude evidence which may be highly cogent and of great assistance to the trier of fact. Consider the following problems: Could defence counsel cross-examine a witness (say, a police informer) on a transcript of a recorded conversation to impugn his recollection of the conversation? Would the accused be barred from introducing a tape recording of a conversation with another person which could raise a doubt as to the accused's own guilt? If the accused denies that any conversation took place as alleged by the police agent, would the Crown be barred from leading a tape recording of that conversation? We believe that any attempt to regulate consent interceptions would be introducing an unnecessary complexity without any real gains in terms of accuracy of fact-finding or protection of legitimate privacy interests.

It should be noted that because of the recommended alteration to the definition of "private communications" it is necessary to expand the exceptions to the offences in *Code* subsection 178.18(1). That section makes it an offence to be in possession of a device knowing that the design thereof renders it primarily useful for "surreptitious

92. *Id.*, vol. 1, paras. 1131-2, p. 49.

93. See: *R.* v. *Lapointe and Sicotte* (1983), 9 C.C.C. (3d) 366 (Ont. C.A.); *R.* v. *Lessard* (1982), 10 C.C.C. (3d) 61 (Qué. C.A.).

interception of private communications.'' Under the *Goldman*[94] formulation, one could never be sure until after the fact whether the communications being tape-recorded by a party to it were private communications, since whether or not a communication was a private communication depended on who the originator was.

Under our proposals, even where one party consents to, or in fact makes, the tape recording (interception), the communication is private if another party to it has a reasonable expectation of privacy. Accordingly, persons in possession of tape recorders designed to record their own conversations without the knowledge of the party could now find themselves liable criminally, depending on the meaning to be attached to the word ''surreptitious.'' We therefore propose an amendment to section 178.18 to clarify that an interception in such circumstances is not unlawful. This would also alleviate the necessity for the proposed amendment in section 25 of Bill C-18 to *Code* section 178.18.[95]

RECOMMENDATIONS

14. That section 178.11 continue to provide that it is not unlawful to intercept private communications where the interception is made with the consent, express or implied, of any party to it.

15. That the offence in subsection 178.18(1) not apply to any person in possession of a device or component for the purpose of using it in an interception made or to be made with the consent of one of the parties.

16. (1) That a peace officer, before commencing an interception under this section, shall inform the person whose consent is sought that he has a right to refuse to consent and to withdraw his consent at any time.

(2) That consent under this section may be given orally or in writing.

17. That the signature of a person on a document warning him of his right to refuse to consent and of his right to withdraw his consent at any time or a recording of such consent be *prima facie* proof of the consent of the person to the interception.

94. *Supra*, note 33.

95. That amendment would add to the list of exemptions from liability paragraph 178.18(2)(*b*.1) as follows:
... 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; ....

II. The Authorization

A. The Application Procedure

Section 178.12 of the *Criminal Code* provides that the application for an authorization is to be made *ex parte* by a designated agent to a Supreme Court judge or a judge as defined by *Code* section 482 which, in provinces which have them, includes a judge of the county or district court. In Québec, the effect of reference to section 482 is also to include provincial court judges. Concern has been expressed that the application is *ex parte*, the only persons present being the judge, the agent and the police officer who swore the affidavit which, pursuant to subsection 178.12(1), must accompany the application. While a similar concern could be raised with respect to the ordinary search warrant procedure, the Supreme Court of Canada has held that such a proceeding may be *in camera*.[96]

It would, of course, defeat the purpose of the application if the proposed target were given notice of the application, but suggestions have been made for the assignment of *amicus curiae* or *amicus publicae* to represent, in a sense, the interests of the proposed target, and presumably the public interest to some extent as well. Cohen has observed that "[s]ecrecy could still be maintained, but the public would gain a measure of added assurance that the privacy interest was receiving more than simple lip-service."[97] The idea of an *amicus publicae* has received little support and, while the concerns which Cohen and others have raised cannot be dismissed, we are not prepared to recommend the establishment of such an institution, provided that our recommendations concerning disclosure of the material used on the application are implemented. Since in the end the *amicus* would be dependent upon the authorities for his information, it is not clear that such an institution would afford a significant or real protection to privacy. We would be concerned that the *amicus* would afford only the illusion of protection and would undermine arguments in favour of implementing the disclosure recommendations which we believe have the potential to afford real protection and accountability.

At present, the *ex parte* hearing is not only *in camera*, but is also not transcribed. There is no court reporter present and no recording is made. Some uncertainty exists as to whether the judge may question the affiant and supplement, by oral testimony, the facts in the affidavit. It has been pointed out that on the renewal application, in addition to the written application and the affidavit, the application may be supported "by such other information as the judge may require." Again, it is not clear in what form this information should be received. This uncertainty can have serious consequences if the recommendations with respect to disclosure are adopted, since the application procedure will be more open, and hence, more open to challenge. While the

96. *Attorney-General of Nova Scotia* v. *MacIntyre*, [1982] 1 S.C.R. 175, 65 C.C.C. (2d) 129.

97. Stanley A. Cohen, *Invasion of Privacy: Police and Electronic Surveillance in Canada* (Toronto: Carswell, 1983), p. 137.

authorizing judges should be encouraged to challenge the material in the affidavit, there must be a record of any statements from the officer which are relied upon to grant the authorization so that they are available when there is a later review. Accordingly, we adopt the same procedure recommended in Working Paper 30 with respect to search and seizure.[98]

RECOMMENDATION

18. That the application for an authorization or renewal continue to be in writing and accompanied by an affidavit of a peace officer. The hearing shall be *ex parte* and *in camera*. The judge should be empowered to place the peace officer under oath to ascertain additional facts underlying the application. However, if such facts are relied upon in the adjudication of the application, a record of such facts shall be included in the sealed packet.

B. Basis for Granting the Authorization

The basis upon which an authorization may be granted is set out in *Code* subsection 178.13(1) and is intended to emphasize the extraordinary nature of the intrusion. The core of the limitation is contained in paragraph (*b*) which requires that the judge be satisfied:

> ... 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.

While to a certain extent this implements the "last resort" criteria which properly attend the use of this method of investigation, it does not address the more nebulous problem of the gravity of the suspected offence. As indicated above, while electronic surveillance was seen as a necessary tool to fight organized crime and other serious crime, in practice its use has never been so restricted. Throughout our consultations, concerns were voiced that electronic surveillance was being misused in the investigation of trivial offences. While we have not cut back significantly on the authorizable offences listed in section 178.1, we still consider that the public interest is best served by the restriction of so intrusive an investigative tool to serious examples of the authorizable offences. Accordingly, we propose amendment to paragraph 178.13(1)(*a*) which presently provides that the judge be satisfied:

> that it would be in the best interest of the administration of justice to do so; ....

98. *Supra*, note 47, pp. 185-8.

RECOMMENDATION

19. That paragraph 178.13(1)(*a*) be amended to provide that the judge may grant an authorization where he is satisfied that it would be in the best interest of the administration of justice and in the public interest having regard to the seriousness of the offence under investigation.

C. Interprovincial Offences

Organized crime and other types of crime do not necessarily respect provincial boundaries. The issue has been raised whether judges in one province have jurisdiction to authorize an interception in another province. To date, the answer seems to be in the negative[99] although in *R.* v. *Bengert*,[100] Berger J. held that the Superior Court could authorize interceptions outside the province. Our view is that, at present, Part IV.1 does not permit such authorizations. Moreover, Osler J. pointed out in *Re Application for Authorization to Intercept Private Communications*, that what is "normally authorized and the conditions under which the authorization may be exercised, may vary considerably from province to province."[101]

Several solutions have been proposed for this problem:

(a) "Backing system" similar to the procedure in *Code* subsection 443(2).

While this solution was favoured by several government representatives, we see serious problems. For example, on what material would the "backing" judge act? Should he review the initial application, or merely rubber-stamp the authorization? What criteria would govern the exercise of his discretion? And what of the police? If the authorization is backed, would they be required to implement the order and perhaps commit scarce resources to a project to which they would ordinarily give a low priority? At the very least, the application to back the authorization would have to be accompanied by an affidavit of a peace officer in the judge's jurisdiction indicating willingness to carry out the order and further indicating that the application has been approved by an agent of the provincial Attorney General or the Solicitor General as the case may be.

(b) Amendment of section 178.13 to give the judge the power to authorize an interception in another province.

We think that the issues raised by Osler J. and set out above, are the appropriate considerations and that this would not be the proper solution.

99. *Supra*, note 76, *per* Bouck J.; and *Re Application for Authorization to Intercept Private Communications* (1983), 9 C.C.C. (3d) 347 (Ont. H.C.J.), *per* Osler J.

100. *R.* v. *Bengert*, [1979] 1 W.W.R. 193 (B.C. S.C.).

101. *Supra*, note 99, p. 349.

(c) Amendment of section 178.13 to give the judge of the Federal Court power to authorize interception anywhere in Canada.

This is not a solution which has found favour with any of the persons consulted. Apart altogether from any other concerns, judges of the Federal Court have not previously been involved with electronic surveillance applications under Part IV.1 and have not been able to develop the necessary expertise. Their involvement in criminal matters generally is rather limited, and it may be imposing an unfair burden to require them to consider these interprovincial applications.

(d) Leave the provisions as they are.

We basically favour leaving matters as they are, subject to one amendment to be discussed below. The various law enforcement agencies did not perceive this as a serious problem, and indicated that as a result of co-operation with other forces they had not encountered serious difficulties.

One problem was brought to our attention which we feel does warrant reform. This is as a result of the present wording of paragraphs 178.12(1)(*a*) and (*b*):

> (1) An application for an authorization shall be made *ex parte* and in writing to a judge of a superior court of criminal jurisdiction, or a judge as defined in section 482 and shall 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, 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, in respect of any other offence in that province, ...

The effect of these provisions is that a judge would seem to have no power to authorize an application where the offence is not being committed or was not committed in the province. Where an offence is committed in one province and the suspects were believed to be living in another province, it would seem that neither province could apply for an authorization. We expect that this is an oversight and that the legislation should be amended to permit authorities in one province to apply for an authorization, notwithstanding that the offence was committed in another. Moreover, such an amendment is consistent with our view that the authorization should primarily be person-oriented.

RECOMMENDATION

20. That subsection 178.12(1) be amended to provide that an authorization may be granted where the communications of the targeted person may be intercepted in one province, although the offence is alleged to have been committed in another province.

D. Minimization

While respect for privacy and restraint should be the important if not governing principles in the execution of such an intrusive investigative device as electronic surveillance, they generally receive minimal attention, once the order is granted. Thus, one of the most difficult challenges to any review of the present legislation is the question of minimization. Minimization is the procedure by which only those communications which are the proper subject of the investigation are intercepted and recorded. Unlike the United States federal legislation, Part IV.1 of the *Criminal Code* contains no explicit minimization requirement. An authorization will name certain persons, specify certain addresses and perhaps telephone numbers. It will as well contain a "basket clause" which permits the interception of unknown persons in contact with the named persons. The lines are ordinarily only monitored for two of three eight-hour shifts. Whether monitored or not, the recording devices operate automatically, recording all calls to and from the number. In addition, when the line is being monitored, a log is kept which sets out a brief summary of each call. Irrelevant calls are often noted as such.

Certain forms of surveillance are more closely monitored. However, even where the device is live monitored there is no policy requiring that irrelevant communications not be recorded.

The authorization in operation acts like a huge electronic vacuum cleaner, indiscriminately sucking in the relevant with the irrelevant without distinction. It has been represented to us by government people and the police that minimization requirements would destroy the effectiveness of wiretapping as an investigative tool. They point to the relative infrequency of use of wiretapping in the United States as a consequence of strict minimization requirements which make wiretapping a costly, inefficient investigative tool. We are not convinced that such is the case, in view of the American case-law to be dealt with *infra*, but it should be pointed out that wiretap legislation was intended to be the tool of last resort because of the serious implications to privacy and liberty. It is not self-evident that the legislation should be drafted to make wiretapping the preferred method of investigation.

Recent case-law has tended to encourage the erosion of what minimization safeguards there are in the legislation as it now exists. For example, in *R.* v. *Samson (No. 6)*,[102] the court considered that it was well within the bounds of a standard authorization to intercept the calls of tradesmen and other casual users of the targeted telephone, since their calls might include messages for the targeted individuals or other pieces of information which may assist in the investigation. So far as we are aware, except for the very rare case (for example, interception of a judge's or a lawyer's calls), the only minimization condition included in most authorizations is to require that visual surveillance accompany any interceptions at public telephones. This condition is not necessarily required by the present legislation, but is included "voluntarily" by the agents. It may be that judges would not otherwise authorize interceptions at public telephones if they were aware the authorization permitted it. (We should point out that a standard clause in most authorizations — the "resort to" clause — permits interceptions at all places, both stationary and mobile, to which the named persons may resort.)

It should be pointed out as well that this is one area where the Charter may have important implications. Additionally, Canada's obligations as a signatory to the United Nations *International Covenant on Civil and Political Rights* are of significance.[103] At the heart of these documents are respect for privacy and an obligation to protect against arbitrary and unreasonable infringements of that privacy. Questions could be raised as to whether it is unreasonable and arbitrary to sanction a system which permits the interception and recording of all telephone calls made to a certain telephone, irrespective of the user or the content of the conversation.

In our view, the key to an appropriate minimization requirement is recognition of the privacy interest. Interception should only be authorized where there is a basis for believing the targeted person is himself involved in criminal activity of the specified kind. We think that it is inconsistent with the Charter, our obligations as signatory to the *International Covenant on Civil and Political Rights* and the principles which should guide criminal procedure to permit widespread intrusions into the privacy of other persons on the tenuous basis that such interceptions may assist in an investigation. On the other hand, it is not necessarily unfair to permit interceptions and recording of all the calls of the named person, notwithstanding that some (even the majority) of these calls may not be "relevant." To require that only "relevant" calls be intercepted and

102. *R.* v. *Samson (No. 6)* (1982), 37 O.R. (2d) 48, 237 (Ont. Co. Ct.), reversed *supra*, note 58.

103. Canada is a signatory to the United Nations *International Covenant on Civil and Political Rights*, which entered into force on March 23, 1976, Article 17(1) of which states:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Both section 8 (unreasonable search and seizure) and section 7 (protection of life, liberty and security of the person) of the Charter recognize privacy as a fundamental attribute of a modern society. Of course, it remains to be seen whether section 7 in particular will be developed to reflect a broad right of privacy enforceable through the courts, as have the Fifth and Fourteenth Amendments in the United States through due process protection of "liberty." Thus, see L. Tribe, *American Constitutional Law* (New York: Foundation Press, 1978), especially Chapter 15: "Rights of Privacy and Personhood," and the discussion in the judgment of Parker A.C.J.H.C. in *R.* v. *Morgentaler, Smoling and Scott* (1984), 14 C.C.C. (3d) 258 (Ont. H.C.J.), pp. 299-314.

recorded may have important implications for the accused's right to make full answer and defence. It may be prejudicial and misleading to have available only the relevant, that is, incriminating part of a much longer conversation. One call taken out of context may have a very different interpretation when placed in the context of other calls by the accused. On the other hand, it places an almost impossible burden on the monitor to anticipate when the conversation will turn to the illegal activity.

To have truly effective minimization, the device would have to be live monitored at all times. While estimates vary, it is probably fair to say that this would at least triple the cost of any investigation. Accordingly, the gains to privacy have to be carefully assessed, and in the end we are not satisfied that the minimal gains to privacy which would accrue from requiring mandatory live monitoring in all cases are worth the immense increase in costs. We illustrate the minimal benefits by reference to the United States experience.

The leading case in the United States is *Scott* v. *United States*.[104] Under Title III[105] section 2518(5), the order must include a clause that the interception "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter." While the order in *Scott* contained such a clause, agents intercepted *all* calls, only forty per cent of which related to the targeted offence (narcotic trafficking). The majority of the court concluded, however, that the minimization requirement was not infringed. The court adopted an objective reasonableness standard, rather than one which depended on an assessment of the police motives or good faith.[106]

If, as in *Scott*, the interception of *all* calls was lawful, even under a regime requiring live monitoring and minimization, then where is the significance or any gain to the privacy interest? Moreover, under any minimization procedure which could be suggested, privacy is still invaded, at least by the monitor. The only gain may be that the conversation is not tape-recorded so there is no permanent record. In our view, a mandatory statutory minimization requirement with mandatory live monitoring of the device is not justified. On the other hand, our consultants were all of the view that it would be helpful to have a list of minimization terms which the authorizing judge could include in the order in much the same way that subsection 663(2) of the *Criminal Code* contains a list of specific terms which a judge may include in a probation order. We believe that this represents a viable and practical solution to a very difficult problem.

A specific aspect of the minimization problem concerns solicitor-client and other privileged communications. As a result of an incident in which the telephone in the barristers' lounge in the Sault Ste. Marie courthouse was wiretapped, subsections (1.1) and (1.2) were added to section 178.13 of the *Criminal Code*. They provide as follows:

104. *Scott* v. *United States*, 436 U.S. 128 (1978).

105. Title III, *supra*, note 67, section 802, 82 *Stat.* 212.

106. See *supra*, note 104, pp. 139-41.

(1.1) No authorization may be given to intercept a private communication at the office or residence of a solicitor, or at any other place ordinarily used by a solicitor and by other solicitors for the purpose of consultation with clients, unless the judge to whom the application is made is satisfied that there are reasonable grounds to believe that the solicitor, any other solicitor practising with him, any person employed by him or any other such solicitor or a member of the solicitor's household has been or is about to become a party to an offence.

(1.2) Where an authorization is given in relation to the interception of private communications at a place described in subsection (1.1), the judge by whom the authorization is given shall include therein such terms and conditions as he considers advisable to protect privileged communications between solicitors and clients.

However, subsection 178.13(1.2) has recently been interpreted in *R.* v. *Chambers*[107] as not imposing any obligation on the judge to impose conditions to protect privileged communications. Anderson J.A., however, considered that "in most cases ... a protective clause should be inserted in the authorization to protect persons other than named targets."[108]

In our view, the intent of subsections (1.1) and (1.2) was to minimize interception of privileged communications, and that in such circumstances conditions must be mandatory.

A related problem concerns interception of privileged communications between a lawyer and client as the result of interceptions on the client's telephone. There is a certain analogy to search and seizure law in this respect. In *Descôteaux* v. *Mierzwinski*[109] the court held that solicitor-client privilege is not simply a rule of evidence, but rather has a much wider scope, and in fact has given rise to a substantive rule.

The rule formulated by Lamer J. proposes that the confidentiality of communications between solicitor and client may be raised in any circumstances where such communications are likely to be disclosed without the client's consent.[110]

While subsection 178.16(5) preserves the privilege with respect to admissibility of evidence, in our view the substantive rule, as formulated by Lamer J., has an implication at the interception stage which should be recognized in the legislation. It should be noted that in the recent case of *R.* v. *Heikel*,[111] Wachowich J. of the Alberta Court of Queen's Bench excluded all the wiretap evidence because of the repeated interception and recording of solicitor-client calls after the accused were first charged, notwithstanding that the Crown did not intend to adduce any of those conversations in evidence. His Lordship also objected to the repeated interception and recording of conversations between two accused who were husband and wife, although such conversations were

107. *R.* v. *Chambers* (1983), 9 C.C.C. (3d) 132 (B.C. C.A.).

108. *Id.*, p. 141.

109. *Descôteaux* v. *Mierzwinski* (1982), 70 C.C.C. (2d) 385, *per* Lamer J. (S.C.C.).

110. *Id.*, p. 400.

111. *R.* v. *Heikel*, Alta. Q.B., May 25, 1984, Wachowich J. (unreported).

also privileged. However, since the spousal communication privilege is strictly an evidentiary one and does not, it seems, give rise to a substantive rule,[112] we do not propose to make mandatory the minimization of such interceptions.

It will be observed that we have not specifically dealt with the consequences of failure to observe any conditions designed to implement minimization requirements imposed by the judge. This has proved an intractable problem in the United States (see, for example, *United States* v. *Dorfman*[113] and *United States* v. *Suquet*[114]). Since we recommend retention of the same admissibility rule as contained in present section 178.16, we see no reason to design special admissibility rules for minimization conditions. It will be for the trial judge to determine whether, in the particular case, the interception was made in accordance with the terms and conditions of the authorization, and thus lawfully made.

RECOMMENDATIONS

21. That an authorization may only be granted in relation to persons the interception of whose private communications will assist in the investigation of the offence by reason of their involvement in the offence.

22. That section 178.13 be amended to provide that the judge, in granting the application, may include any of the following terms and conditions:

(a) that the device be live monitored at all times that it is proposed to intercept or record private communications;

(b) that so far as is reasonably possible, only the conversations of targeted persons be intercepted and recorded;

(c) that where it is proposed to intercept communications at a telephone to which the public has a right of access, then any interceptions shall be on the basis of live monitoring and accompanied by visual surveillance;

(d) that reasonable steps be taken not to intercept private communications between spouses, physician and patient or persons in other confidential relationships;

(e) that reasonable steps be taken not to intercept private communications of targeted persons which by reason of a known pattern are unlikely to assist in the investigation of the offence;

(f) that interception cease after the object of the investigation has been obtained;

(g) that, where the interception of a telephone line will involve a party line, no interception occur except when the line is being monitored;

112. See: *Rumping* v. *Director of Public Prosecutions*, [1962] 3 All E.R. 256 (H.L.); *R.* v. *Kotapski* (1984), 13 C.C.C. (3d) 185 (Qué. C.A.).

113. *United States* v. *Dorfman*, 542 F.Supp. 345 (1982) (N.D. Ill.), appeal dismissed, 690 F.2d 1217.

114. *United States* v. *Suquet*, 547 F.Supp. 1034 (1982).

(h) such further terms and conditions as the judge considers advisable to minimize the acquiring and recording of private communications which would not assist in the investigation.

23. That the authorization shall include a term requiring that, where an interception is to occur at a place mentioned in subsection 178.13(1.1), reasonable steps shall be taken to ensure that privileged communications between solicitors and clients are neither intercepted nor recorded.

24. That where there are grounds to suspect that if an authorization is granted, privileged communications between the targeted person and his solicitor will be intercepted, that fact shall be disclosed in the application to obtain an authorization.

25. That in a case to which Recommendation 21 applies, the authorization shall include a term that, so far as reasonably possible, privileged communications between the targeted person and his counsel not be intercepted or recorded.

E. Basket Clauses

In *R.* v. *Welsh and Iannuzzi (No. 6)*,[115] the implications of failing to provide for the interception of unnamed individuals became apparent — the evidence of their conversations was inadmissible, since the interception had not been lawfully made. It has since been standard to include in an authorization a "basket clause" permitting the interception of communications of unknown persons. It should be pointed out that the basket clause is required only where the communication is between two persons neither of whom is named in the authorization. If at least one of the participants is named, then the interception is authorized and lawful, barring bad-faith concealment of the identity of one of the participants.[116]

The clauses that are included vary widely but are intended to meet the problem of getting before the courts the communications which were intercepted of persons who were not named in the authorization. The main point of litigation has become identifying the scope of the basket clause. It is often argued that the accused was known to the police at the time the authorization was obtained, and therefore interception of his calls was not authorized in a clause providing for "unknowns." It seems to us, however, that in terms of protecting privacy, this debate has few implications. This was also the view of the Supreme Court of the United States in *Donovan*.[117]

The issue from the privacy perspective is: To what extent should the law sanction and permit interceptions of persons who are not identified with the offence at the time

115. *Supra*, note 31.

116. *R.* v. *Gill* (1980), 56 C.C.C. (2d) 169 (B.C. C.A.).

117. *United States* v. *Donovan*, 429 U.S. 413 (1977).

the authorization is obtained? The problem also arises because of the threshold condition before which an individual is targeted, namely, any person "... the interception of whose private communications there are reasonable and probable grounds to believe may assist the investigation of the offence, ..."[118]

If electronic surveillance is considered a search or seizure within the meaning of section 8 of the *Canadian Charter of Rights and Freedoms*, then a statute which authorizes an unlimited basket clause may, to that extent, be unreasonable. In the United States, the consitutionality of Title III has been upheld in the lower courts, and by implication in the Supreme Court in *Donovan*. These cases focused on whether the legislation meets the requirements of the "warrant clause" of the Fourth Amendment.

In our view, this is not a satisfactory approach in the Canadian context. As Carr points out in *The Law of Electronic Surveillance*[119] the search warrant analogy is not very apt.

More to the point, in the Canadian context, is the absence of a warrant clause in section 8. While the Supreme Court of Canada has nevertheless held that there is a presumption in favour of a warrant as a prerequisite to a reasonable search,[120] it is not clear that there is a presumption in favour of any particular form of warrant.

There must be some provision, however, for unknown persons. These fall into two classes: (1) persons believed to be involved in the offence but unidentifiable; and (2) persons who are not only unidentified but whose existence may be wholly speculative at the time of the authorization. An example can be given to illustrate the two classes. Consider a narcotics investigation.

While it may be legitimate to permit the interception of conversations of any of these people, drafting legislation to permit such interceptions poses serious problems. A widely drafted basket clause becomes an invitation to indiscriminate interceptions and invasion of privacy. While some basket clauses are drafted so as to require a link between the offences, for example, "all persons, presently unknown resorting to certain premises for the purposes of committing one of the named offences," many are not, for example, "all persons found to be communicating with the named individuals at the specified premises."

While in our view the privacy interest could only be vindicated by a basket clause that would limit the interception to the conversations of persons of a class believed to be involved in the offence, this can create serious difficulties not only in drafting the clause but in its implementation. For example, one basket clause in common use in Ontario was as follows:

118. *Criminal Code*, s. 178.12(1)(*e*).

119. Carr, *supra*, note 67 (Supp., 1983), pp. 3-4.

120. *Supra*, note 37.

(3)(b) Authorization is also hereby given to intercept the private communications of persons whose identities are presently unknown, in accordance with the terms of this Authorization, provided that there are reasonable and probable grounds to believe that the interception of such private communications may assist the investigation of any of the offences stated in paragraph 1 above, whether or not any such person described in paragraph 3(a) above is party to such private communications.[121]

In other words, the clause repeated the test set out in paragraph 178.12(1)(*e*) of the *Criminal Code*, and as found by the Ontario Court of Appeal in *R.* v. *Paterson, Ackworth and Kovach*[122] was an unlawful delegation of the judge's function to the police. It was pointed out that it is the judge's function to determine the class of persons whose private communications may be intercepted under a basket clause. In our view, this is the correct approach. Furthermore, the judge must ensure that the basket clause is drafted so as to identify the appropriate group of persons, such as: permanent residents of the premises; habitual visitors believed to be involved in the offence; and so on. We believe that our recommendations are consistent with the interpretation in the *Paterson* case.

In our view, a basket clause is only legitimate if it permits the interception of the conversations of persons of a class known to be involved in the offence. Accordingly, a basket clause must be no wider than to permit interception of persons believed to be involved in the offence but unidentified at the time of the obtaining of the authorization.

Consistent with our view as to the proper scope of the interception, the threshold condition for targeting persons (known and identified) as presently contained in *Code* paragraph 178.12(1)(*e*) must be modified so as to replace the "assist in the investigation" requirement with a requirement of involvement in the offence as set out above in Recommendation 21.

One further concern about basket clauses is the use of a clause which permits installation of a device at other than named premises. When combined with a wide basket clause as to persons, one authorization can become very sweeping. While the need for the authorities to be able to respond quickly to changing locations is legitimate, this should be limited to the named persons to keep the scope of the authorization within reasonable bounds.

However, to avoid impediments to legitimate law enforcement objectives and yet improve judicial scrutiny, we believe there should be provision for the agent to return to the authorizing judge to obtain his approval of the wider use of the basket clause. Allied to this is a recommendation that the legislation direct the judge's attention to his right to insert a condition in the authorization requiring periodic reports as to the operation of the investigation. We do not envisage this as a normal condition but it

121. Excerpt of an authorization made by Judge McCart on June 10, 1982, and cited in *Paterson*, *infra*, note 122, p. 147.

122. *R.* v. *Paterson, Ackworth and Kovach* (1985), 18 C.C.C. (3d) 137.

may well be considered appropriate in certain sensitive investigations. Aside from these recommendations, we believe that *Code* sections 178.12 and 178.13 should remain as they are in respect of the granting of the original authorization.

RECOMMENDATIONS

26. That subject to Recommendation 27, the authorization shall contain a clause naming or otherwise identifying the persons the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence by reason of their involvement in the offence.

27. That, in addition, the authorization may contain a clause permitting the interception of a class of unidentified persons whose private communications there are reasonable grounds to believe may assist the investigation of the offence by reason of their involvement in the offence.

28. That subject to Recommendation 29, the authorization shall limit the interceptions to specified premises.

29. That the authorization may contain a clause permitting interception of private communications at other than specified premises where the other place is resorted to by persons known and identified in the authorization. At such premises, only those communications to which the known and identified person is a party may be intercepted, unless the specially designated agent has applied in writing to the authorizing judge as soon as practicable for amendment of the authorization. The application for an amendment shall be supported by the affidavit of a peace officer setting out the reasons for interception at these premises, the names of the persons whose communications are likely to be intercepted and the reasons why interception at such premises is required. The judge may refuse to amend the order, or amend the order, which amendment is effective from the date when interception commenced at the additional premises, unless the judge is not satisfied that the application was made as soon as practicable, in which case the amendment may be made effective at such later date as the judge sees fit in the circumstances.

30. That the legislation contain a list of terms or conditions which *may* be included in the authorization, such as the following:

(a) that periodic reports be made to the authorizing judge as to the identities of persons whose communications are being intercepted pursuant to a basket clause;

(b) that periodic reports be made to the authorizing judge as to the places, not specifically named in the authorization, where interceptions are taking place.

F. Surreptitious Entry

By surreptitious entry, we mean the physical entry into private premises by law enforcement agents without the consent or knowledge of the occupier, for the purpose of installing a listening device. In the usual case, this means installation of a radio transmitter capable of transmitting oral communications to a location outside the premises where the communications can be recorded. While surreptitious entry may be used in some cases solely to install a device to assist in intercepting telephone communications, this is usually unnecessary and accordingly unusual. As a result of the decisions of the Supreme Court of Canada in *Lyons* v. *The Queen*[123] and *Wiretap Reference*[124] released on December 20, 1984, the present legal position may be summarized as follows:

(a) Unless the authorization contains limitations on or prohibition of surreptitious entry, an authorization by necessary implication authorizes any person acting under the authorization to enter any place at which private communications are to be intercepted to install or to service a permitted listening device, provided such entry is required to implement the authorization.

(b) The process of interception includes the installation of the device, and therefore an interception is only lawfully made within the meaning of paragraph 178.16(1)(*a*) if the installation was lawful.

(c) However, lawful means in accordance with Part IV.1, and therefore a surreptitious entry to install a device to implement an authorization being lawful, the interception would be lawfully made.

The McDonald Commission[125] favoured legislation with express power to authorize surreptitious entry in the national security field. This had two elements: first, the right to enter must be explicit and subject to certain limitations; and secondly, it must be permitted by a judge only in certain circumstances.

The Commission also made recommendations in the criminal investigation field, convinced that surreptitious entry was legitimate for the purposes of electronic surveillance[126] although not for search and seizure generally.[127] As indicated above, it was the McDonald Commission's view that surreptitious entry was not legal at present. Its Recommendation 265 is as follows:

WE RECOMMEND THAT section 178.13 of the Criminal Code be amended to permit peace officers executing authorizations under this section to take such steps as are reasonably

123. *Lyons* v. *The Queen*, [1984] 2 S.C.R. 631.

124. *Wiretap Reference*, [1984] 2 S.C.R. 697.

125. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Mr. Justice D.C. McDonald, Chairman, *Freedom and Security under the Law* (Second Report, 2 volumes) (Ottawa: Minister of Supply and Services Canada, 1981) (hereinafter cited as the McDonald Report).

126. *Id.*, vol. 2, pp. 1022-3.

127. *Id.*, vol. 1, p. 144; vol. 2, p. 1019.

necessary to enter premises or to remove property for the purpose of examining the premises or property prior to installing a device or for the purpose of installing, maintaining or removing an interception device, providing the judge issuing the authorization sets out in the authorization

(a) the methods which may be used in executing it;

(b) that there be nothing done that shall cause significant damage to the premises that remains unrepaired;

(c) that there be no use of physical force or the threat of such force against any person.[128]

The Commission also noted that in the United States, despite a decision of the United States Supreme Court holding that surreptitious entry was lawful, constitutional legislation was under consideration to control surreptitious entry. The McDonald Commission referred to the evidence of the Assistant Attorney General, Criminal Division, before the Senate Judiciary Committee, wherein it was observed that:

> In the United States, despite the affirmation by the Supreme Court of the implied power of entry, the government has introduced a bill before the Congress which *expressly* provides for entry and for procedural safeguards to ensure that such methods will be used only when, as the Assistant Attorney General, Criminal Division, has said, "such methods have been found reasonable and necessary by an informed, impartial judicial officer."[129]

Moreover, notwithstanding the United States Supreme Court decision, it is the policy of the United States Justice Department to seek specific judicial authorization for a surreptitious entry.

The one dissenting voice in this area, as to the need for legislation, is the report prepared by the McLeod Committee[130] in response to the McDonald Report. The McLeod Committee was of the view that surreptitious entry was lawful and that legislation was not necessary to govern the area. While, as it turned out, the McLeod Commitee was right in concluding that surreptitious entry was not unlawful, for reasons set out below we are of the view that if surreptitious entry is to be permitted, it must be specifically dealt with by the legislation.

As indicated above, one of the cases that went to the Supreme Court originated as a reference directed to the Alberta Court of Appeal.[131] In the Court of Appeal, Chief Justice McGillivray and Justice Harrandence were of the view that surreptitious entry was lawful only if specifically authorized by the judge in the authorization. Both Justices saw the need for judicial control through appropriate conditions.[132]

128. *Id.*, vol. 2, p. 1023, Recommendation 265.

129. *Id.*, vol. 1, p. 175.

130. Federal/Provincial Committee of Criminal Justice Officials, *Report to Deputy Ministers of Justice, Deputy Attorneys General and Deputy Solicitors General by the Federal/Provincial Committee of Criminal Justice Officials with Respect to the McDonald Commission Report*, R.M. McLeod, Q.C., Chairman (Ottawa: Communications Division, Solicitor General of Canada, 1983) (hereinafter cited as the McLeod Committee Report).

131. *Reference re an Application for an Authorization* (1983), 10 C.C.C. (3d) 1 (Alta. C.A.).

132. See the comments of Chief Justice McGillivray, *id.*, pp. 14-5.

Mr. Justice Harrandence specified the conditions when surreptitious entry should be authorized:

> I am of opinion that if a superior court judge, on an application for an authorization made pursuant to Part IV.1 of the *Criminal Code*, determines that the public can *only* be served by the interception of private communications and that effective interception of those communications can *only* be obtained by placing a device on private property, then it is his duty to adapt the common law to meet modern conditions by authorizing a surreptitious entry or a suitable strategem to effect the installation of a device on that property.[133] [Emphasis in original]

The same concerns are echoed in the majority judgment in *Lyons* v. *The Queen* where Estey J., while holding the right of entry need not be explicit in the authorization, went on to recommend that it was a matter that should be considered by the authorizing judge.

> Having regard to the pattern of Part IV.1, the breadth of authority granted to the court, the importance of the subject-matter, and the vitality of the role of the court in the legislative plan as the guardian of the public interest, explicit response by the court to the application for authority to intercept in many cases will require the prescription of "terms and conditions advisable in the public interest" pursuant to para. (2)(*d*) of s. 178.13.[134]

Further, in *The Criminal Law in Canadian Society*[135] the position taken is that "the criminal law should provide and clearly define powers necessary to facilitate the conduct of criminal investigations." The Law Reform Commission has previously considered the problem of surreptitious entry.

In the Search and Seizure Working Paper, the Commission recommended that "[m]odifying search and seizure procedures to accommodate surreptitious police intrusions would result in serious sacrifices of the protective features of these procedures," and that "[a]bsent compelling evidence of the need for such sacrifices, the modifications should not be made in the context of criminal or crime-related investigations."[136]

It was pointed out that neither at common law nor by statute was surreptitious entry authorized for search and seizure. The Search and Seizure Working Paper essentially addressed the problem of intelligence probes and did not purport to deal with electronic surveillance. Nevertheless, the standard suggested for an exception may be appropriate, namely, Is there compelling evidence of the need for surreptitious entry in the area of electronic surveillance?

The figures that are available are ambiguous and unreliable in the attempt to determine whether surreptitious entry is necessary. Certainly it is probably fair to say that surreptitious entry is a relatively rare event. That is not surprising. Surreptitious entry

133. *Id.*, p. 28.

134. *Supra*, note 123, p. 671.

135. *Supra*, note 35, p. 61.

136. *Supra*, note 47, Recommendation 42, p. 260.

involves certain risks to the investigation. The officers may be caught installing the devices, or the devices may be discovered. Surreptitious entry may, as well, be difficult and involve expenditure of time and effort which can only be justified where there is a significant probability that evidence will be obtained which could not be obtained by the easier wiretap method. Nevertheless, surreptitious entry has been used in the electronic surveillance field and used effectively. Other devices such as parabolic microphones are not only less effective, but represent a greater likelihood of intrusion into the communications of innocent parties.

In Working Paper 30, two important problems were identified with surreptitious entry in the area of search and seizure. First, such entry was often justified in circumstances where grounds for a search warrant did not yet exist. This would not be a problem in the electronic surveillance area, since the entry would only be justified as a means of implementing the authorization. While some instances exist of police covertly entering premises to consider the feasibility of implanting microphones, this intelligence-gathering function cannot be justified independent of a judicial decision that grounds for an authorization to intercept private communications exist. As pointed out in Working Paper 30, "[t]o permit exploratory entries to ascertain whether such grounds exist is to render protection against unjustified intrusion extremely tenuous."[137]

A second problem identified in Working Paper 30 is that of reviewability and accountability. This is a serious problem in a regime of search and seizure which depends on announcement of entry, provision of documents to the occupier and allowing the occupant to witness the search. Modifications of these rules "would severely compromise the degree of protection associated with warrant procedure ...."[138] Again, however, there are not similar concerns in the electronic surveillance field. Even telephone wiretaps as presently authorized are done secretly and are quite different from the normal search and seizure. The policy decision to permit electronic surveillance is really a decision to permit the investigation to proceed in secrecy or covertly. The real issue in the electronic surveillance field is, What forms of secret intrusion should we permit and with what safeguards? This is not to discount the accountability problem but, as pointed out in Working Paper 30, it is a problem which pervades the electronic surveillance area.[139]

Since we favour a somewhat more open regime generally, some of these concerns will be addressed. Certainly, with respect to surreptitious entry, a special form of notification may be appropriate where no charges are laid and so reviewability and accountability through the trial process are not available. In its project on *Minimum Standards for Criminal Justice, Standards Relating to Electronic Surveillance,* the American Bar Association considered this problem and concluded:

> Inventory procedures can thus be worked out which would eliminate the most serious aspects of the objection to the surreptitious character of electronic surveillance: it needs, in short, to be surreptitious only initially. This objection, too, need not be controlling.[140]

137. *Id.*, p. 266.

138. *Id.*, p. 267.

139. *Id.*, p. 268.

140. *Supra*, note 50, p. 92.

But what of the privacy interest? How grave an intrusion is surreptitious entry? The entry itself is not meant to be discovered and therefore is ordinarily done with as little disturbance as possible, although this is not always the case.[141] The real intrusion is into the occupier's privacy subsequently, as a result of the capability of the device to pick up communications in the privacy of home or office, as indicated by Chief Justice McGillivray[142] in *Reference re an Application for an Authorization*, and Justice Estey in the *Lyons*[143] appeal.

Private thoughts are disclosed in home or office with no idea that they would even be disclosed in a telephone conversation. Since it represents such a serious intrusion into privacy, surreptitious entry to implant listening devices should only be permitted in very carefully circumscribed circumstances.

At the least, the right to make such entry should not be implied in every authorization, but must be the subject of prior judicial approval on the basis that, having regard to the seriousness of the particular offence and the likelihood of obtaining evidence, such an intrusion is justified. Further, conditions as suggested by the McDonald Commission in its proposed National Security Act would have to be imposed.

The recent Supreme Court decisions, however, did not deal with any implications which section 8 of the *Canadian Charter of Rights and Freedoms* might have for surreptitious entry.

It should also be pointed out that in *Dalia* v. *United States*,[144] the court found no infringement of the Fourth Amendment. In *Dalia*, the warrant had authorized interception of all oral communications "at the business office" of Dalia. The court concluded that by implication this was an authorization to make a covert entry which was not an unconstitutional infringement of the Fourth Amendment. The court was strongly of the view that Congress clearly understood that it was conferring power upon the courts to authorize covert entries ancillary to their responsibility to review and approve wiretap applications. By analogy to search warrants, there is no constitutional requirement that the electronic surveillance warrant set out the means by which it is to be executed.

We believe that the decision of the Supreme Court of Canada in *Hunter* v. *Southam Inc.*,[145] with its strong preference for prior judicial authorization to comply with section 8 of the Charter, strongly favours a statutory regime where the right to make surreptitious entry is explicit both in the legislation and in the authorization.[146]

141. There are apparently examples where a fire-alam was set off in order to empty the premises and provide access to the authorities to plant the device.

142. *Supra*, note 131, p. 12.

143. *Supra*, note 123.

144. *Dalia* v. *United States*, 441 U.S. 238 (1979).

145. *Supra*, note 37.

146. It is perhaps worth noting that Dickson C.J.C., who wrote the judgment of the court in *Southam*, *supra*, note 37, dissented in both *Lyons*, *supra*, note 123, and the *Wiretap Reference*, *supra*, note 124, being of the view that Part IV.1 of the *Code* did not permit surreptitious entry. Even the McLeod Committee Report conceded that the Charter could pose problems for covert entry.

A broad consensus emerged in our consultations that there was no basis upon which to limit the availability of surreptitious entry to certain serious offences, and that it was a matter that should be left for the individual judge to consider within certain guidelines. Nevertheless, in our view, surreptitious entry ought to be reserved for serious cases where there exists substantial likelihood that relevant evidence will be obtained.

We are firmly of the view that entry should only be effected in reliance on the authorization granted under Part IV.1 and should not be made by reliance on some other legal process such as a search warrant. As the Ontario Court of Appeal in *R.* v. *McCafferty* [147] pointed out, a search warrant must be strictly interpreted, and cannot be used to carry out a general search or used to plant a listening device.

Similarly, an entry under authority of an authorization is not authority to conduct a search of the premises although windfall information obtained during a covert entry could be the basis of an application for a search warrant to be executed in the normal manner.

A system of prior authorization depends, of course, on disclosure, to the authorizing judge, that the police will seek to use covert entry. We have been concerned as to the extent of disclosure required, and in particular, whether the means to be used to enter ought to be disclosed. It was forcefully represented to us that on the one hand there is a need for flexibility since the police may have to adapt their methods to changing conditions, and that on the other hand the judge lacking the necessary technical expertise would not likely be in a position to assess properly the viability or even desirability of one method over another. The concern, however, is over the use of inappropriate means to make the entry, such as sounding a false fire-alarm to clear the building. After considerable discussion, we have decided to opt for greater flexibility and not to require that the particular method to be used be disclosed in the application. If, in subsequent years, there should be abuse of the power, this position will of course have to be reconsidered, but at present we have no good reason to be concerned. We would, however, give the authorizing judge the power to deal specifically with certain means of entry if he considers it desirable.

RECOMMENDATIONS

31. That the authorizing judge be given power to authorize an entry onto private premises without the consent of the occupier, for the installation, removal or servicing of an electromagnetic, acoustic, mechanical or other device.

32. That the authorizing judge may only so authorize where the circumstances of the offence are serious and there is a high degree of likelihood that relevant evidence will be obtained.

147. *R.* v. *McCafferty* (1984), 13 W.C.B. 143 (Ont. C.A.).

33. That an application for an authorization which includes an authorization to make a surreptitious entry shall state the reasons why such entry is required and why other less intrusive means will not be sufficient.

34. That it be an offence to enter private premises without the consent of the occupier for the purpose of installing, servicing or removing an electromagnetic, acoustic, mechanical or other device without an order under Part IV.1 of the *Criminal Code*, and an offence to remove anything from the premises at the time of the entry.

35. That the peace officer making the entry should not be entitled to use force against any person for the purpose of effecting such entry or exit, except as necessary to protect himself or others.

36. That the authorizing judge may order that certain means be used/not used to effect the entry.

37. That following the investigation, the owner and occupier of the premises be notified of the entry and be given a copy of the order which authorized the entry.

38. That reasonable steps be taken to repair any damage to the premises or to compensate the owner for any significant damage left unrepaired.

39. That the use of a small amount of electricity to enable the device to function shall not constitute a criminal offence.

G. Renewals

The intrusiveness of electronic surveillance also arises from the length of time during which the intrusion takes place. For some investigations, the interception may extend over a period of many months. The *Criminal Law Amendment Act, 1977* extended the length of authorizations from thirty to sixty days.[148] While *Criminal Code* paragraph 178.13(2)(*e*) provides that the order may be valid for a period "not exceeding" sixty days, in fact, it is only on the very rare occasion that any order is for less than sixty days. By comparison, the United States legislation[149] provides for a maximum of thirty days and requires that the order contain a termination clause, that is, that the interception not continue for any period longer than is necessary to achieve the objective of the authorization. The average length of the American authorizations seems to vary from state to state and even county to county, but in most jurisdictions it approaches the

148. *Criminal Law Amendment Act, 1977*, S.C. 1976-77, c. 53, s. 9(3).

149. Title III, *supra*, note 67, s. 2518(4) and (5).

maximum permitted by statute. The efficacy of the termination clause is less than clear since, generally, the device is operated for the full term authorized.[150] (There are no statistics required by section 178.22 of the *Criminal Code* as to the duration of the interception.)

The Canadian legislation permits renewals or extensions for sixty-day periods.[151] The obvious purpose of a time-limit on the authorization is to place more temporal restraint on the interception to prevent the authorization from becoming an open-ended type of general warrant. Provision for a renewal or extension recognizes that some investigations may legitimately take longer than sixty days. However, consistent with the principle of restraint, there must be a demonstrated need for this further intrusion.

However, as the result of recent case-law, police rarely seek a renewal of an authorization. Rather, a new authorization will be sought even if only very minor changes are contemplated. In *R.* v. *Badovinac*,[152] the court held that a renewal could only extend the time of the original authorization but it could not "extend, modify, add to or otherwise deal with any feature of the authorization."[153] As pointed out in *R.* v. *Pleich*,[154] there are certain implications to legislation which favours obtaining a new authorization rather than a renewal. While on balance the requirements for an authorization set out in section 178.12 may be more onerous than the requirements for a renewal, it is those latter requirements which are really directed to the desirability of permitting the continuation of a wiretap investigation beyond the statutory limit. Subsection 178.13(3) provides for renewal of an authorization (1) upon an *ex parte* application, (2) accompanied by an affidavit of a peace officer or public officer deposing to the following matters, namely: the reason and period for which the renewal is required; full particulars of interceptions and information obtained; and the number of instances an application for renewal was made, withdrawn or refused — and (3) supported by such other information as the judge may require.[155]

While, as pointed out in *R.* v. *Pleich*,[156] the full and frank disclosure expected on an application under section 178.12 for a subsequent authorization would likely require the kind of information referred to in subsection 178.16(3), it is not statutory.

In our view, the legislation must be modified so that renewals are available where only minor changes are contemplated to the original authorization but the same investigation is being pursued. On the other hand, where the investigation has developed to the point where significant changes are needed, then a new authorization is appropriate.

150. *Report on Applications for Orders Authorizing or Approving the Interception of Wire or Oral Communications, 1983* (Washington, D.C.: Administrative Office of the United States Courts, 1983) (hereinafter cited as the Wiretap Report).

151. *Criminal Code*, s. 178.13(4).

152. *R.* v. *Badovinac* (1977), 34 C.C.C. (2d) 65 (Ont. C.A.).

153. *Id.*, p. 70.

154. *R.* v. *Pleich* (1980), 55 C.C.C. (2d) 13 (Ont. C.A.).

155. *Criminal Code*, s. 178.13(3).

156. *Supra*, note 154.

However, in the latter case there must be full disclosure of the extent of the prior investigation, so that the judge is in a position to consider the merits of the application properly.

We are also of the view that the longer the investigation, the greater intrusion, and hence the need for greater judicial scrutiny and responsibility upon the law enforcement officials. Accordingly, we propose that the normal term of a renewal be thirty days, unless grounds are shown for the longer period of up to sixty days. We believe that such an approach is more consistent with the principle of restraint. Of course, steps must be taken to ensure that the police have not applied for an authorization to take advantage of the longer period.

RECOMMENDATIONS

40. That where, to the knowledge of the designated agent or the deponent of the affidavit made in support of an authorization, an authorization has previously been granted in relation to the same or a related investigation, the application shall contain the information referred to in paragraph 178.13(3)(*b*) of the *Code*.

41. That a renewal of an authorization may include the names of persons previously provided for in the authorization but unnamed in the authorization.

42. That a renewal of an authorization may include additional places of interception of persons provided for in the original authorization.

43. That minor variations of the terms of the authorization may be included in a renewal, including the following:

(a) different or more accurate descriptions of persons or places;

(b) different or additional means of interception;

(c) different or additional offences clearly related to the offences in the original authorization and part of the same investigation.

44. That a renewal of an authorization may include terms not included in the original authorization, designed to minimize interceptions of communications which are not related to the offence.

45. That a renewal shall be for a period not exceeding thirty days, with the exception that where special cause is shown, a renewal may be for a period not exceeding sixty days. "Special cause" in this recommendation means circumstances making it probable that the investigation will not be completed within thirty days *and* it would be impracticable to obtain a further renewal within thirty days. Where the period of a renewal exceeds thirty days, the judge shall indicate on the face of the authorization the reasons therefor, with reference to the particular circumstances of the investigation.

46. That in any case referred to in Recommendation 45, the judge shall ensure that a renewal would not be available in the circumstances. In no case shall an authorization be granted where there is reason to suspect that it is intended to avoid the effect of Recommendation 45. Where the only reason that a renewal is unavailable is because the previous renewal or authorization has expired, then the subsequent authorization shall be for thirty days, unless special cause has been shown.

47. That the legislation provide for a list of terms and conditions which may be included in the renewal such as the following:

(a) that the interception shall terminate once the objective of the original authorization is achieved;

(b) that any applications for subsequent renewals or authorizations be made to the judge who granted the original authorization or renewal.

III. Reviewability and Secrecy

A. Introduction

While it is a fundamental feature of the Anglo-Canadian judicial system that judicial acts be open and subject to scrutiny by the public and higher courts, a feature which has now taken on constitutional dimensions,[157] another significant feature of Part IV.1 has been the lack of openness in the application process and judicial reticence to review subsquently the propriety of the application. Crown and police consultants have consistently represented to us that the internal controls in the application process, the necessity that the request for an authorization be reviewed by senior law enforcement officials and then by Crown counsel, ensure that only meritorious applications are brought forward. This, however, particularly in the case of such an intrusive means of investigation, misses the point, as Mr. Justice Jackson said in *Johnson* v. *United States*[158] in relation to the Fourth Amendment protection against unreasonable search and seizure. Such judgments should be made by a neutral and detached magistrate rather than an officer engaged in the actual investigation.[159]

It might well be asked, however, that the importance of involvement of the disinterested judicial official at the application stage having been accepted as a crucial element in securing the public from unreasonable invasion of privacy, What reason is

157. Paragraph 2(*b*) of the *Canadian Charter of Rights and Freedoms* as interpreted in *Re Southam Inc. and The Queen (No. 1)* (1983), 3 C.C.C. (3d) 515 (Ont. C.A.).

158. *Johnson* v. *United States*, 333 U.S. 10 (1948) (referred to in *supra*, note 46).

159. *Id.*, pp. 13-4.

there for further judicial scrutiny at the time it is sought to admit the evidence? The arguments in favour of openness after the execution of a search warrant have been made by Dickson J. in *Attorney-General of Nova Scotia* v. *MacIntyre*.[160] The point, it seems, is accountability to ensure against abuse of the very sweeping and intrusive powers placed in the hands of the police through search warrant and wiretap procedures. It would be ideal, perhaps, if every wiretap order could be subjected to subsequent judicial scrutiny to determine whether there has been abuse. This, however, is not practicable and is probably of little real benefit in gauging the likelihood of abuse. The fact is that essentially only in the context of the criminal trial process, where the liberty of the individual is at stake, are the resources available to scrutinize these procedures properly. It is only at that stage that the subject of the invasion has a sufficient interest and information to challenge the procedure, and the state a sufficient interest to defend properly the action taken by the authorities. Thus, the criminal trial process serves as the ultimate guardian of security of the privacy interest. The prospect that the actions will be subject to the intense scrutiny of the criminal trial protects the integrity of the entire system and shields the public generally from unreasonable invasion. There are, of course, costs associated with greater scrutiny: trials may be longer; police investigative techniques may be disclosed; "guilty" persons may be set free. The problem is to balance the privacy interests with these costs, recognizing that in view of these costs, the criminal trial process is an "inefficient" means of scrutinizing the functioning of the investigative process generally and especially in the area of electronic surveillance.

B. Review of the Authorization

The present provisions of the *Criminal Code* do not explicitly set out the grounds for review of the authorization. Review of the authorization is, of course, tied to the admissibility of evidence. While it may be that civil remedies could be sought for improper interceptions, the important questions arise in the context of the criminal trial process.

The threshold condition for admissibility of evidence in *Code* paragraph 178.16(1)(*a*) is that the interception was lawfully made. (There is also provision for admission by consent of one of the parties in paragraph 178.16(1)(*b*) but this involves different issues.) This paragraph roughly corresponds to section 2515 of Title III. Courts have construed this paragraph as permitting the admission of evidence where one of the parties to the communication consents to the interception so that it is not unlawful by reason of *Code* paragraph 178.11(2)(*a*).[161] The other ground for a lawful interception in paragraph 178.11(2)(*b*) is where the person "intercepts a private communication in accordance with an authorization ...." This requires that the Crown establish that the police were not only acting under an authorization, but that interception of the particular communication was authorized by the terms or conditions of the authorization. When the

160. *Supra*, note 96, pp. 144-7 (C.C.C.).

161. *Supra*, note 33.

legislation was first enacted, authorizations were not always as widely drafted as they are now, and the language used was not always as precise as it might have been. One of the first appellate decisions is a good example of an interception that was not made in accordance with the authorization. In *R.* v. *Welsh and Iannuzzi (No. 6)*,[162] it was held that an interception was not lawfully made when neither of the parties to the communication were named in the authorization, or otherwise provided for in the authorization. Another example is *R.* v. *Niles*.[163] These cases simply require the judge to look at the authorization and determine whether the particular interception fits within it.

These cases, however, shade into more difficult problems which raise issues as to the reviewability of the authorization. For example, where the authorization names certain persons as targets and also includes a basket clause for unknown persons, what of an accused who is unnamed but alleges he was known at the time the authorization was obtained? This can be looked at in two ways. On the one hand, the accused is not provided for on the face of the authorization: he is unnamed, yet not unknown so as to fall within the basket clause. This seems to have been the view of the Ontario Court of Appeal in *R.* v. *Crease (No. 2)*.[164] On the other hand, this also seems to be going behind the authorization. In order to determine whether the accused was meant to be included as an unknown for the purposes of the basket clause, the trial judge would need access to the secret packet so as to determine what material was before the authorizing judge. On its face, the authorization permits the interception of the accused as an unknown person. This approach essentially equates unknown with unnamed, and is not entirely persuasive. It was, however, accepted by the majority of the British Columbia Court of Appeal in *R.* v. *Lloyd and Lloyd*.[165] It should be noted that, in the *Lloyd* case, there was no allegation of fraud or wilful nondisclosure.

The known/unknown problem can shade into a true question of going behind the authorization. For example, where the allegation of the accused is not merely that he was "known" at the time the authorization was obtained, but that his identity was not revealed to the authorizing judge, deliberately, because had the judge known of the police intention to intercept his communications (either under the basket clause or as party to a communication with a named person), the authorization would not have been granted. In *R.* v. *Gill*,[166] the evidence obtained was held to be inadmissible after the judge found that the police had concealed their intention to intercept the communication of the unnamed person and that they intended to intercept the communication between the accused (who was named) and the unnamed person in the jail after the arrest of the accused. The court of appeal held that none of the conversations between the two were admissible in view of the defects in the obtaining of the authorization. It is interesting that the court's approach was not to determine whether the authorization was

162. *Supra*, note 31, pp. 13-4 (O.R.), p. 375 (C.C.C.).

163. *R.* v. *Niles* (1978), 40 C.C.C. (2d) 512 (Ont. C.A.).

164. *R.* v. *Crease (No. 2)* (1980), 53 C.C.C. (2d) 378 (Ont. C.A.).

165. *R.* v. *Lloyd and Lloyd* (1980), 53 C.C.C. (2d) 121, 16 C.R. (3d) 221, (B.C. C.A.), reversed in part on other grounds (1982), 64 C.C.C. (2d) 169, 131 D.L.R. (3d) 112, 39 N.R. 474 (S.C.C.).

166. *Supra*, note 116, p. 176.

rendered void, voidable or unenforceable, but merely to treat the question solely as one of admissibility. The court, in ruling the communication inadmissible, relied on the wording of former paragraph 178.16(2)(*b*) which, like the present subsection 178.16(3), refers in an oblique way to substantive defects (as opposed to defects in form) in the application for the authorization.

The other issue which clearly presents a reviewability problem is raised in *Wilson* v. *The Queen*.[167] In that case, the trial judge found a substantive defect in the application based on evidence at trial that led him to conclude that none of the pre-conditions in paragraph 178.13(1)(*b*) had been met. He arrived at his conclusion solely on the basis of *viva voce* evidence without examining the sealed packet. All members of the court considered that he was in fact going behind (reviewing) the authorization and that the procedure was improper. The court divided, however, on the proper procedure. The majority *per* McIntyre J. essentially disagreed with the *Gill* approach and held that subsection 178.16(3) gives no jurisdiction to exclude evidence for substantive defects where the interception was made in accordance with an authorization, valid on its face. By implication, however (and by analogy to civil cases where *ex parte* orders are granted), where the authorization was improperly obtained it can be set aside by the authorizing judge. Presumably then, any interception which had been made pursuant to the now invalid authorization would be retroactively rendered unlawful and the communication inadmissible.

In his minority judgment, Dickson J. would permit collateral attacks to the authorization by the trial judge, but considered that the trial judge erred in holding that he did not need to consider the contents of the sealed packet to determine whether there was a defect in the application for the authorization.

Under either scheme, the procedure contemplated is a cumbersome one. If the attack on the authorization must be made before the authorizing judge, this may entail substantial delay and interruption of ongoing trials. Even under the procedure suggested by Justice Dickson, there will be delay if, as in *Wilson*, the trial is before a provincial court judge who has no power to open the sealed packet under section 178.14 of the *Code*.

Other problems relate to the grounds for review or setting aside the order, the pre-conditions, if any, before which the sealed packet can be opened, and if there is a burden on the accused to establish a defect in the application, how to discharge the burden without access to the sealed packet.

McIntyre J., in referring to civil cases, appears to consider "fraud or the discovery of new evidence" as grounds for setting aside the *ex parte* order. In referring to the possibility of another judge of the same court hearing the review due to the exigencies of court administration, he stated: "... the reviewing judge must not substitute his discretion for that of the authorizing judge. Only if the facts upon which the authorization was granted are found to be different from the facts proved on the *ex parte*

167. *Wilson* v. *The Queen* (1983), 9 C.C.C. (3d) 97 (S.C.C.).

review should the authorization be disturbed."[168] One might well ask where the evidence of different facts is to come from. The majority judgment raises the spectre of lengthy preliminary hearings in an effort to discover new facts as a foundation for the review.

In his concurring judgment, Mr. Justice Dickson did not enumerate the grounds for review of validity, but noted the cases which have refused access to the sealed packet except where there is a *prima facie* case of fraud or nondisclosure, to which he added misleading disclosure. He appears to contemplate that the grounds for review could emerge during cross-examination at trial of the deponent of the affidavit.[169]

Again however, the spectre of undue waste of time is raised. Defence counsel under the scheme are required to conduct a fishing expedition. They must grope around in the dark hoping to turn up something which gets them into the sealed packet, without knowing what that something even looks like.

The final area of review is noted by Dickson J. This is facial invalidity. For example, the authorization fails to specify the period for which it is in force, or the date when it was granted. It is to these perhaps technical defects which the curative provision in subsection 178.16(3) appears directed.

The problems presented by review in particular, going behind the authorization, are serious and fundamental from a position both of policy and procedure. In our view, these problems can only be overcome by a clear statement as to the grounds and procedure for review and access to material.

American courts have had a somewhat longer and different experience under Title III and a survey of that experience may prove helpful. Sections 2518(9) and (1)(a) of Title III contemplate much freer access to material than is the case under Part IV.1. Section 2518(10)(a) also sets out the grounds for "suppression" of the evidence:

> Any aggrieved person in any trial, hearing or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire or oral communication, or evidence derived therefrom, on the grounds that —
>
> (i) the communication was unlawfully intercepted;
>
> (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or
>
> (iii) the interception was not made in conformity with the order of authorization or approval.[170]

The question of review really revolves around ground (i). In *United States* v. *Giordano*,[171] the court considered the meaning of "unlawfully intercepted" in (i) and concluded that the words are not limited to constitutional amendments, as:

168. *Id.*, p. 97.

169. *Id.*, p. 112.

170. Title III, *supra*, note 67, s. 2518(10)(a).

171. *United States* v. *Giordano*, 416 U.S. 505 (1974).

> Congress intended to require suppression where there is failure to satisfy any of those statutory requirements that directly and substantially implement the congressional intention to limit the use of intercept procedures to those situations calling for the employment of this extraordinary investigative device.[172]

Subsequent litigation has turned on what requirements were designed to "directly and substantially implement" the congressional intent, or put another way, which provisions "play a central role in the statutory scheme."[173]

C. Fishman, in his text, *Wiretapping and Eavesdropping*, has compiled a list on "central" and "non-central" provisions as follows:[174]

Central

1. AUTHORIZING OFFICIAL: 18 USCS s. 2516(1) (federal) and (2) (state).
2. DESIGNATED OFFENSES: 18 USCS s. 2516(1) (federal) and (2) (state).
3. PROBABLE CAUSE: 18 USCS ss. 2518(1)(b)(i-iii) and 2518(3)(a,b,d).
4. NORMAL INVESTIGATIVE PROCEDURES: 18 USCS s. 2518(1)(c) and (3)(c).
5. THIRTY-DAY MAXIMUM PERIOD: 18 USCS s. 2518(5).
6. TERMINATE UPON ATTAINMENT OF AUTHORIZED OBJECTIVE: 18 USCS s. 2518(4)(e) and (5).
7. PRIOR APPLICATIONS: 18 USCS s. 2518 (1)(e).

Non-Central

1. IDENTIFYING THE AUTHORIZATION OFFICIAL: 18 USCS s. 2518(1)(a) and (4)(d).
2. IDENTIFYING THE TARGETS IN THE APPLICATION: 18 USCS s. 2518(1)(b)(iv).
3. IDENTIFYING THE TARGETS IN THE WARRANT: 18 USCS s. 2518(4)(a).
4. INVENTORY AND NOTICE: 18 USCS s. 2518(8)(d).

Numbers (3) and (4) of the "central" provisions and numbers (2) and (3) of the "non-central" provisions, require most careful scrutiny, since they are the grounds which could arise or have arisen under the Canadian legislation. In this area, the leading case is *United States* v. *Donovan*,[175] which held that:

> [A] wiretap application must name an individual if the Government has probable cause to believe that the individual is engaged in the criminal activity under investigation and expects to intercept the individual's conversations over the targeted telephone.[176]

This was in accord with the earlier decision in *United States* v. *Kahn*.[177]

172. *Id.*, p. 527.

173. *Id.*, p. 528.

174. C.S. Fishman, *Wiretapping and Eavesdropping* (Rochester, N.Y.: The Lawyers Cooperative Publishing Co., 1978), pp. 372-6.

175. *Supra*, note 117.

176. *Id.*, p. 428.

177. *United States* v. *Kahn*, 415 U.S. 143 (1974), p. 155. The court then rejected a requirement that the order identify all persons whom the government could have discovered by diligent investigation.

It was held that section 2518(10)(a)(i) did not require suppression of Donovan's conversations. The court took a somewhat practical approach, asking the question whether it would have made a difference to the authorizing judge.[178]

The reasoning in *Donovan* demonstrates why, if the probable cause for the normal investigative procedures requirements is not met, the evidence would be suppressed. Clearly, if the judge knew that, for example *per* section 2518(3)(c), normal investigative procedures have been tried and have succeeded, he would not have been empowered to grant the warrant. Moreover, the section 2518(3) requirements, like the *Code* subsection 178.13(1) requirements, underpin the congressional/parliamentary intent to limit the resort to this extraordinary and highly intrusive method of investigation.

Certainly, the *Donovan* approach is sufficient to vindicate the restraint principle. The question remains, Is it sufficient to vindicate the privacy interest? We think that it probably is. On the other hand, the investigation into known/unknown does not really advance the privacy interests, except in the case where it could be said that the judge would not or could not have granted the authorization, had he known the true scope of the intended targets (*Gill*[179]), or had he known the possibility of indiscriminate interception of "unknown" targets. We think this latter problem is one of minimization and can often involve very fine distinctions. Where it is apparent that the authorization would be granted for the primary targets, it hardly advances the protection of privacy to require the police to *include*, as targeted individuals, persons who may be only marginally involved because failure to do so might invalidate the authorization. This will simply have the effect of enlarging the scope of the wiretap investigation rather than restraining it. Where an apparent primary target is not identified, then an inference of oblique motive would arise and would be properly dealt with under the rubric of *Gill*-type reasoning.

As noted above, section 2518(10)(a) of Title III gives as a third ground for suppression that the interception was not made in conformity with the order of authorization. This is similar to the way *Code* paragraph 178.16(1)(*a*) has been interpreted and poses no new problems.

Since *Wilson*, there have been a few decisions by authorizing judges who have been asked to set aside their orders. To date, no firm principles have emerged as to when the judge will be prepared to: (1) open the packet; or (2) set aside the order. In *R.* v. *Delhaye*,[180] O'Leary J. opened the packet and set aside the order, it seems, simply because he found that the affidavit had not disclosed the identities of two of the parties, the interception of whose conversations there were reasonable and probable grounds to believe would assist the investigation. That seems a drastic result. There is nothing in the judgment to indicate that this omission was done in bad faith (as *per Gill*), nor any reasoning as to why the entire order was set aside. Significantly, O'Leary J. did not ask himself the question whether he would have granted the order knowing the true

178. *Supra*, note 117, p. 435.

179. *Supra*, note 116.

180. *R.* v. *Delhaye*, Ont. H.C.J., March 7, 1984, O'Leary J. (unreported).

state of affairs: (a) as it was; (b) including the two individuals; (c) specifically excluding the two individuals as targets; (d) not at all. This may well be because of the lack of any guidance in *Wilson*[181] as to when the authorization may be set aside, except for the rather unhelpful comment by McIntyre J., referred to earlier, based on cases dealing with setting aside *ex parte* orders in civil cases.

In another post-*Wilson* case, *R.* v. *Con and Fung*,[182] another practical problem with the *Wilson* procedure was pointed out. In that case, the authorizing judge, Huddart Co.Ct.J., was asked to make findings as to the state of knowledge of the police about the identity of one of the conspirators and the availability of other normal investigatory techniques, based upon testimony adduced in other proceedings. Some of the evidence was conflicting and required findings of credibility. His Honour observed that he was "at a considerable disadvantage in assessing the weight to give to [the investigating officer's] evidence." Judge Huddart was also confronted with the problem as to when he was justified in opening the packet on the basis of an allegation that at least one of the criteria in paragraph 178.13(1)(*b*) had not been met. He concluded that this was not sufficient, as there must be *prima facie* evidence on all three criteria before the sealed packet is opened, or alternatively, there must be evidence of deliberate deception with regard to one of the criteria. The fact that one criterion has not been met is not sufficient.[183]

C. Secrecy

Closely allied to the problem of reviewability is that of access to materials. *Code* section 178.14 contains quite exceptional provisions for keeping the material filed on the application secret, by placing it in a sealed packet to be kept in the custody of the court, and to be opened only for the purpose of dealing with an application for renewal or pursuant to an order of a judge referred to in the section.[184]

While subparagraph 178.14(1)(*a*)(ii) gives a section 482 judge power to open the packet, that jurisdiction has been narrowly construed. A representative case is *Re Stewart and The Queen*[185] where Mr. Justice Krever held that the power to open the sealed packet "is a power to be reserved for the exceptional case"[186] and that the "circumstances must be rare"[187] when the jurisdiction would be exercised.

181. *Supra*, note 167.
182. *R.* v. *Con and Fung* (1984), 11 C.C.C. (3d) 396 (B.C. Co.Ct.).
183. *Id.*, p. 404.
184. *Criminal Code*, s. 178.14(1).
185. *Re Stewart and The Queen* (1976), 30 C.C.C. (2d) 391 (Ont. H.C.J.).
186. *Id.*, p. 401.
187. *Id.*, p. 402.

While Krever J. did not articulate the grounds which *would* justify an order under subparagraph 178.14(1)(*a*)(ii), other cases such as *Re Royal Commission Inquiry into the Activities of Royal American Shows Inc. (No. 3)*,[188] have limited the circumstances to those of fraud and similar misconduct by the authorities.

Section 178.14 also stands in the way of a person who has been the object of an interception and so notified under section 178.23, but not charged. That person is virtually cut off in any attempt to challenge the legality of the authorized interception by the secrecy provisions.[189]

The grounds for opening the packet paralleled the grounds for reviewing the authorization in the pre-*Wilson* cases. As Zuber J.A. indicated in *R.* v. *Welsh and Iannuzzi (No. 6)*,[190] such grounds "would include cases in which the authorization was defective on its face, or was vitiated by reason of having been obtained by a fraud."[191]

An authorization can only be set aside on the basis of fraud or wilful nondisclosure. To ascertain whether there has been fraud or wilful nondisclosure, the defence needs access to the sealed packet, but to gain access it must show fraud or wilful nondisclosure. The way that some counsel have attempted to break the circle is to cross-examine the police officer who made the affidavit. The logical inconsistency of this tactic has not escaped the courts. Thus, in *R.* v. *Haslam*,[192] it was held that the officer could not be cross-examined on the contents of the affidavit in the absence of an order under *Code* section 178.14. Leaving for a moment the question of review, the secrecy provisions raise other problems:

(a) limited empirical data as to the scope of basket clauses;

(b) virtually no data as to whether the statutory prerequisites in fact existed — for example, that other investigative measures had been tried and had failed;

(c) virtually no data as to whether basket clauses are in fact resorted to for the interceptions;

(d) virtually no data as to whether monitoring of the devices takes place;

(e) virtually no means of determining the seriousness of the case in which the interceptions take place.

These are primarily problems of openness and accountability and the Law Reform Commission is on record as favouring to the greatest extent possible openness and reviewability of the conduct of law enforcement agencies. An argument favouring

188. *Re Royal Commission Inquiry into the Activities of Royal American Shows Inc. (No. 3)* (1978), 40 C.C.C. (2d) 212 (Alta. S.C.), p. 219.

189. *Re Zaduk and The Queen* (1979), 46 C.C.C. (2d) 327 (Ont. C.A.). This particular problem is discussed *infra* under the heading "VI. B. Notice under Section 178.23."

190. *Supra*, note 31.

191. *Id.*, pp. 371-2 (C.C.C.).

192. *R.* v. *Haslam* (1977), 36 C.C.C. (2d) 250 (Nfld. Dist. Ct.).

' openness' in respect of judicial acts was forcefully put by Dickson J. in *Attorney-General of Nova Scotia* v. *MacIntyre*[193] in relation to search warrants, and can also be applied to other areas of police powers.

Mr. Justice Dickson went on to indicate that the concern for accountability is not diminished by the fact that the search warrants might be issued by a justice *in camera*, but, rather "this fact increases the policy argument in favour of accessibility." He indicated that "what should be sought is maximum accountability and accessibility but not to the extent of harming the innocent or of impairing the efficiency of the search warrant as a weapon in society's never-ending fight against crime," and concluded that "curtailment of public accessibility can only be justified where there is present the need to protect social values of superordinate importance. One of these is the protection of the innocent."[194]

The question then is whether, in the field of electronic surveillance, secrecy is required to "protect social values of superordinate importance." Two values have been identified by the police and government representatives: protection of informers, and protection of police investigative techniques. It has also been forcefully put to us that the present system of confidentiality encourages greater candour in the material before the authorizing judge, and that if there were a more open regime, police and agents would be less likely to place the entire picture before the judge for his consideration. This last issue is an important one where the *only* method of accountability is the prior judicial approval. It is less important if other post-interception review procedures exist. This is not to discount the importance of this consideration, but it may be somewhat exaggerated, as evidenced by the experience of the McDonald Commission.[195]

What then are the societal values on the other side of the issue?

1. *Restraint*: The very high proportion of authorizations granted as compared to those of the United States leads to the conclusion that authorizations are applied for in circumstances where the crimes under investigation are not serious and other methods of investigation would be more appropriate — that is, there is an unjustified pervasiveness of a very intrusive device.

2. *Accountability*: There is essentially no check on the truth of the material filed in support of the application after the granting of the authorization.

3. *Review*: Opportunities by the accused to test the lawfulness of the application are essentially frustrated.

4. Individuals who have not been charged but have been targeted are prevented from testing the lawfulness of the application and the interception in civil courts.

193. *Supra*, note 96.

194. *Id.*, pp. 144-7 (C.C.C.).

195. Supra, note 125, vol. 2, pp. 1021-2.

D. Conclusion

As indicated above, the problems of review and secrecy are closely related and any solution to the reviewability issues depends on the degree of access to materials. It was therefore proposed that we adopt a procedure whereby the accused would be given complete access to the material used on the application, as is done in the United States. The viability of this procedure was presented to our consultants and there was almost complete agreement that, subject to a method to protect the identity of informers and persons assisting the police, there was no reason not to give the defence complete disclosure. The consultants were frank in stating that they saw no serious problems in terms of disclosure of police investigative techniques. They did not envisage any significant chilling effect on the quality of the material which would be presented on the application. While concerns were expressed that the names of suspects who were never charged would be disclosed, on balance it was felt that the gains in terms of accountability, and even trial efficiency, more than outweigh these problems. As it was pointed out, even under the present system the identity of persons named in the authorization is disclosed during the trial even if some of those persons are not charged. One further concern expressed was the problem that disclosure might interfere with other ongoing but related investigations. However, the consensus was that this would hardly ever be a problem and that, when the issue arose, the Crown would simply have to make the decision as to whether and when to lay charges. This is a problem which is not unique to electronic surveillance, and a special rule could not be justified. The problem of police informers is different. They have always enjoyed special status and protection which has been reaffirmed in very explicit and almost absolute terms by the Supreme Court of Canada.[196] As well, there is a real potential of personal danger to the informant should his identity be disclosed. A solution adopted in the United States is to attempt to draft the material used in the application so as to shield the identity of the informer. We favour a much more direct approach by providing for an *ex parte* application to a judge to seal or delete portions of the affidavit.

Finally, concerns were raised about disclosing the identity of persons who, while not true informers, agree to assist the police on a promise of confidentiality. An example was given of a home owner who may permit the police to use his house as a surveillance point. It was suggested that in certain cases it may be necessary to disclose that person's identity in the affidavit to obtain the authorization, but no real interest was served by disclosing the identity publicly. Since these cases are roughly analogous to cases of police informers, we feel that they too could properly be brought within the procedure for sealing portions of the material. The question then is, When and how should review of the authorization take place, and what are the consequences of that review? The *Wilson*[197] application seems totally unsatisfactory. It can result in substantial delay and disruption of the orderly trial process. Since reviewability of the authorization is tied

196. See, for example: *Bisaillon* v. *Keable* (1983), 7 C.C.C. (3d) 385, 2 D.L.R. (4th) 193 (S.C.C.); *The Solicitor General of Canada* v. *The Royal Commission of Inquiry into Confidentiality of Health Records in Ontario*, [1981] 2 S.C.R. 494, 62 C.C.C. (2d) 193.

197. *Supra*, note 167.

to admissibility of evidence, it should be handled at the trial or preliminary inquiry as the case may be. Broadly speaking, there are two categories which could be grounds for review of the application process: mistake and fraud.

By "mistake" we mean that the judge erred in granting the authorization because on its face there were not sufficient grounds set out in the application upon which a judge, acting judicially, could have made the order. By "fraud" we mean that while the application and affidavit are valid on their face, evidence is available to demonstrate that the facts are not as represented in the affidavit, or there has been wilful omission of pertinent facts. Theoretically, either basis could be grounds for holding that there has been such a defect in the application procedure as to require a sanction. The issue is, however, whether the appropriate sanction is inadmissibility of evidence in both cases. For reasons developed *infra*, under the heading "V. Remedies," we have determined that only the "fraud" category is a sufficient basis for exclusion of evidence. It follows therefore that reviewability of the application process must be limited to those grounds. Other civil remedies for the individual may be available or have to be fashioned where an authorization is mistakenly granted for insufficient reason. Aside from that, we would like to see a review after several years by a panel of experts to determine whether there has been compliance with the provisions of *Code* sections 178.12 and 178.13. With the more liberal disclosure provisions, such a review would now be possible.

If we accept that evidence will be inadmissible where there is a substantive defect in the application as defined *infra* (that is, broadly speaking for fraud), the issues then become merely procedural.

(1) Issue One: Where Is the Question Resolved?

One of the consistent criticisms of the wiretap legislation has been the length of the *voir dire* proceedings to resolve questions of admissibility. Thus, if at all possible, this ground for review should not add appreciably to the length of the proceedings; multiplicity of proceedings should be avoided. On the other hand, we think it will be a rare case where an evidentiary hearing will be required to resolve these issues in view of the definition of substantive defect in the application. A determination at the preliminary inquiry may seem a waste of judicial time. The finding does not bind either party in any subsequent proceedings.[198] On the other hand, an accused has the right to make full answer and defence at the preliminary inquiry and traditionally, the same evidentiary rules have applied at the preliminary inquiry as at the trial.[199] An accused could justifiably complain that he should not be put to the expense and embarrassment of a trial if the only evidence against him is inadmissible. These are all very cogent arguments, and in the end a policy choice must be made. Because we do not believe

198. *R.* v. *Duhamel* (1984), 57 N.R. 162 (S.C.C.).

199. *R.* v. *Pickett* (1975), 28 C.C.C. (2d) 297 (Ont. C.A.); *Re Stillo and The Queen* (1981), 60 C.C.C. (2d) 243 (Ont. C.A.).

that the hearing required will unduly protract the proceedings, we have opted for permitting a challenge to the application procedure to be made at the preliminary inquiry and at the trial.

(2) Issue Two: How Is the Question Resolved?

By reason of the proposed amendment to section 178.14, the accused will have access to almost all of the material used on the application. He can then review that material with his legal advisers and, after conducting whatever investigation he feels appropriate, consider whether there is any basis for challenging the material on grounds of fraud or recklessness on the part of the authorities (the test for inadmissibility as set out in Recommendation 63). In our view, there is an onus on the accused at least to make the issue of a substantive defect a live one before he is entitled to an evidentiary hearing at which the police officers would be compellable witnesses. We would contemplate that the foundation for an evidentiary hearing could be laid by affidavit evidence, which would not, however, be admissible against the accused on the trial proper.[200] The judge would be required to determine whether there is a sufficient basis to conduct a further evidentiary hearing. Obviously, if the affidavit material merely reveals inaccuracies of trifling significance, which could in no way raise a real question as to the integrity of the application procedure, then there would be no basis for ordering a further hearing.

However, where the material raises a real question as to whether there has been a substantive defect in the application, then there must be a full inquiry by the judge. In view of the nature of the grounds of admissibility, we believe that the burden of proof is properly on the Crown to demonstrate the integrity of the application process. It will have complete access to the files and the personnel involved, and be in the best position to lead evidence to resolve the issues properly.[201]

RECOMMENDATIONS

48. That section 178.14 of the *Criminal Code* be amended to include the following:

(a) in addition to the exceptions provided for in present paragraph (1)(*a*), to allow access to the material in the sealed packet for the purpose of dealing with an application for an authorization in related investigations;

(b) to permit the specially designated agent to retain a true copy of all the documents relating to an application made pursuant to section 178.12 or subsection 178.13(3).

200. A similar rule seems to apply with respect to an accused's *voir dire* testimony. See *Erven* v. *The Queen* (1978), 44 C.C.C. (2d) 76 (S.C.C.).

201. The procedure suggested is similar to the comparable American procedure. See Carr, *supra*, note 67, pp. 349-50; *Franks* v. *Delaware*, 438 U.S. 154 (1978); *United States* v. *Licavoli*, 604 F.2d 613 (1979) (9th Cir.).

49. That the prosecutor, when giving notice under subsection 178.16(4), shall include: a copy of the authorization and renewals under which the interceptions were made; and, subject to the order of a court, a copy of all the documents relating to an application for the authorization or renewal.

50. That prior to giving notice pursuant to subsection 178.16(4), the specially designated agent may apply to a judge as defined in section 482 of the *Criminal Code ex parte* and *in camera* for an order that certain portions of the material not be disclosed on the basis that disclosure could tend to reveal the identity of an informer or of any other person who has assisted with the investigation and in the latter case it is shown that it would not be contrary to the public interest that the identity of such persons be withheld. The application should be in writing and supported by the affidavit of a peace officer.

51. That the person against whom evidence is sought to be admitted pursuant to paragraph 178.16(1)(*a*) of the *Criminal Code* by reason of an interception made pursuant to an authorization or renewal, may apply at the preliminary inquiry or the trial to exclude that evidence and derivative evidence on the basis of a substantive defect in the application for the authorization or renewal. The following procedure would apply:

(a) The application should be in writing and supported by affidavit evidence (or *viva voce* evidence with leave of the judge).

(b) Only if the application and the evidence in support when considered together with the material disclosed under Recommendation 49 raises a real question as to whether there is a substantive defect in the application as defined in Recommendation 62 which could lead to the exclusion of evidence, shall the judge hold an inquiry as to the validity of the application for the authorization or renewal.

(c) Should the judge direct an inquiry, the burden of proof is on the Crown to satisfy the court that there was no substantive defect in the application as defined in Recommendation 62.

(d) The affidavit and testimony of the accused is not admissible at the instance of the Crown at the preliminary hearing or trial.

IV. Emergency Authorization: Section 178.15

A problem under the emergency authorization procedure which was drawn to our attention was that of the kidnap victim. It would seem that there is a desire among some law enforcement agencies to be in a position to conduct electronic surveillance immediately should they learn the whereabouts of the kidnap victim, without even having to resort to the emergency procedure under section 178.15. It was suggested that such interceptions could be rendered lawful by deeming the victim of the offence to have consented to any interceptions. On the whole, it is not clear to us that this

would advance the situation, since it is unlikely that the victim would be party to many conversations. Interception of communications to the person who is the victim of extortion would already be lawful, if done with the actual consent of that person. In the one reported case which makes any reference to this issue, *R.* v. *Gamble and Nichols*,[202] it would seem that the police did have time to obtain an authorization (which, however, was held to be defective).[203] In our view, all that is required is a slight modification of section 178.15 to provide some lead time to the police in these very dangerous situations.

A further problem with section 178.15 is the absence of a record of what has taken place. While subsection 178.15(2) requires that the authorization be in writing, there is no requirement that the application be in writing. In the result, it is virtually impossible to review the application subsequently. In our view, particularly in light of our recommendations concerning disclosure, it is desirable that there be some record of the application; for this purpose, the telewarrant procedure, as proposed in section 70 of Bill C-18 which would add section 443.1 to the *Criminal Code*, would appear to be the simplest and most effective mechanism for recording the facts relied upon by the judge in granting the authorization. The facts which would be required to be set out would be: the reasons for resorting to the emergency procedure; the grounds for seeking authorization to intercept; and, the persons and places sought to be intercepted. In our view, this is the minimum record necessary.

RECOMMENDATIONS

52. That section 178.15 be amended by the addition of subsection (6) as follows:

> **The admissibility of evidence acquired as a result of an order obtained under this section is not affected by the fact that the electromagnetic, acoustic, mechanical or other device was installed prior to the obtaining of the order, where the order under this section was obtained in relation to the offence under subsection 247(1) (kidnapping) and no private communications were acquired through use of the device until the order was obtained.**

53. That an application for an emergency authorization under section 178.15 shall be made in writing or by telephone or other means of telecommunication and there shall be a record including: a statement of the reasons why an authorization could not, with reasonable diligence, be obtained under section 178.13; the facts relied upon to justify the belief that an authorization should be given, together with particulars of the offence; the persons whose private communications it is sought to intercept; and, the places of interception.

202. *R.* v. *Gamble and Nichols* (1978), 40 C.C.C. (2d) 415 (Alta. S.C. A.D.).

203. *Id.*, pp. 423-4.

V. Remedies

A. Admissibility of Evidence of Other Offences

It is the nature of electronic surveillance that evidence of other offences than those set out in the authorization may be intercepted. This is particularly the case in a system which does not require minimization as it relates to the subject-matter of the conversation. There are several problems which arise in this area as follows:

1. Ought the law distinguish between unanticipated or "windfall" evidence and evidence which could be foreseen?

2. In either case, do we need a system for obtaining authorization for the new offence or other offences?

3. How do we treat the admissibility of such evidence?

4. What about evidence of offences for which no authorization could have been obtained?

Let us consider first the question of windfall evidence. There is an analogy in this respect to search and seizure, where it is generally accepted that evidence is lawfully (constitutionally) seized if it is uncovered during a lawful search for other evidence in circumstances under which the finding of the new evidence was unanticipated. This is simply a particular application of what is called the plain view doctrine in United States Fourth Amendment jurisprudence.[204]

Where the evidence is unanticipated, no serious policy issues arise. No privacy interest is seriously threatened, since the invasion of privacy has already been legitimately authorized for other reasons.

The integrity of the legislative scheme is also not endangered by permitting the authorities to use such evidence. To the contrary, to refuse to use the evidence could have serious effects on the perception of the legitimacy of the scheme, as indicated in *United States* v. *Cox*.[205]

Questions of policy arise when the evidence of other offences is anticipated. In such circumstances, privacy interests are at stake and the integrity of the legislative scheme is threatened. The underlying assumption of wiretap legislation is a reluctant acceptance that in certain carefully defined circumstances, serious invasions of privacy

204. *Coolidge* v. *New Hampshire*, 403 U.S. 443 (1971); *Texas* v. *Brown*, 103 S.Ct. 1535 (1983); The doctrine is recognized at common law: *Chic Fashions (West Wales) Ltd.* v. *Jones*, [1968] 2 Q.B. 299 (C.A.).

205. *United States* v. *Cox*, 449 F.2d 679 (1971) (10th Cir.), pp. 686-7.

are to be countenanced. At the heart of the scheme is that such serious intrusions will only be permitted for the investigation of certain offences. Ideally, the offences for which wiretapping will be permitted have been selected only after a most delicate balancing of interests. The legitimacy of the entire process is threatened if an authorization is obtained in relation to one offence as a cover for other offences, which may or may not be offences for which an authorization could be obtained (subterfuge interceptions).

The primary control in this area must either be judicial, through the application procedure, or at the stage of admissibility of evidence. Unfortunately, there is no basis for any confidence that the necessary control can be achieved at the authorization application stage; thus, we believe that the application procedure must be structured so that the necessary control can be exercised at the stage of admissibility of evidence. In our view, the only effective way to guard against subterfuge interceptions is to require a showing of good faith at the *voir dire* during the trial whenever it is sought to introduce evidence at the trial of offences not named in the authorization. This additional burden on the Crown will encourage complete disclosure at the application stage, since there will be an incentive to obtain an authorization which names all the offences for which an authorization can be obtained. It will also discourage attempts to obtain authorizations as a means of obtaining evidence of other offences for which an authorization could not be obtained. In our view, good faith in this context would include the following:

(a) that at the time of the authorization or renewal application, evidence of offences other than those specified in the application could not reasonably have been anticipated;

(b) that where evidence of other offences was anticipated, such offences were not named in the application because they were not offences for which an authorization could be obtained *and* they were not the primary focus of the investigation but *only incidental* to an investigation into offences named in the authorization;

(c) that at the time of the application or renewal, disclosure was made to the judge of the authorities to whom it was intended to give information obtained from the interception (this could be an important clue to the true motives and good faith of the authorities — for example, disclosure that it was intended to pass on information to tax authorities may shed light on the real focus of the investigation[206]);

(d) that where the evidence is in relation to an offence for which an authorization could have been obtained and there were suspicions that evidence of such offences would be obtained, those suspicions were disclosed in the material in support of the application *and* those offences were not named in the authorization only because: (i) the grounds for suspicions were not strong enough to meet the statutory test; and (ii) the investigation of such offences was not the primary focus of the investigation but *only incidental* to the primary investigation.

206. See the judgment of Anderson J.A. in *R.* v. *Chambers*, *supra*, note 107.

In our view, these are reasonable safeguards and not out of line with the decisions of the Supreme Court of Canada in *R.* v. *Commisso*.[207] Although that case turned primarily on the interpretation of *Code* subsection 178.16(3.1), both the majority and the dissent touched on the question of good faith. In his dissent, Dickson J. stated that an authorization is obtained in bad faith "where the police, although investigating both the specified and unspecified offences, were primarily interested in the unspecified offence for which they could not get an authorization."[208]

In our view, failure to meet the statutory good-faith test can be considered grounds for exclusion of the evidence. Failure of a showing of good faith is in essence evidence of an attempt to defeat the legislative scheme and privacy safeguards. To admit the evidence in such circumstances could bring the administration of justice into disrepute.

RECOMMENDATIONS

54. That where the prosecution seeks to adduce primary evidence obtained by means of an authorization at the preliminary inquiry or trial of offences none of which are named in the authorization, the judge shall conduct a *voir dire* for the purpose of determining whether the interception of evidence of such offences was done in good faith.

55. That for the purposes of Recommendation 54, "good faith" means:

(a) that at the time of the authorization or renewal application, evidence of offences other than those specified in the application could not reasonably have been anticipated;

(b) that where evidence of other offences was anticipated, such offences were not named in the application because they were not offences for which an authorization could be obtained *and* they were not the primary focus of the investigation but *only incidental* to an investigation into offences named in the authorization;

(c) that at the time of the application or renewal, disclosure was made to the judge of the authorities to whom it was intended to give information obtained from the interception;

(d) that where the evidence is in relation to an offence for which an authorization could have been obtained and there were suspicions that evidence of such offences would be obtained, those suspicions were disclosed in the material in support of the application *and* those offences were not named in the authorization only because

(i) the grounds for suspicions were not strong enough to meet the statutory test,

(ii) the investigation of such offences was not the primary focus of the investigation but *only incidental* to the primary investigation.

207. *R.* v. *Commisso* (1983), 7 C.C.C. (3d) 1 (S.C.C.).

208. *Id.*, p. 11.

56. That where he is not satisfied that the interception of other offences was done in good faith, the judge shall exclude primary evidence and may exclude evidence shown to be derivative, where he is satisfied that to permit such evidence to be adduced would bring the administration of justice into disrepute.

B. For Breach of the Statutory Scheme

(1) Introduction

As part of the Police Powers Project, the Law Reform Commission has been concerned with appropriate sanctions, where the rules as they may be enacted in legislative form, are not complied with by the agents of the state. Enactment of subsection 24(2) of the *Canadian Charter of Rights and Freedoms* has focused attention on exclusion of evidence as the appropriate enforcement mechanism. Not unnaturally, the Commission has considered variants on the rule set out in subsection 24(2) as the test for exclusion of evidence, and rules have been derived which can be found in the Reports on *Questioning Suspects*[209] and *Investigative Tests*.[210] As is apparent from the ensuing discussion, the test for exclusion of evidence in the area of electronic surveillance is different, being both stricter in some respects and more liberal in other respects, particularly as regards defects in the application procedure. It may be that, at a later date, an effort will be made to achieve a uniform rule, but at this stage we are satisfied that the different exclusionary rule for electronic surveillance can be justified.

In the first place, it must be recognized that unlike other aspects of the Police Powers Project, when we came to review electronic surveillance there was already in place a strict exclusionary rule with respect to primary evidence (the communication itself) and a looser exclusionary rule with respect to derivative evidence, not unlike the rule in subsection 24(2) of the Charter. It is to be remembered as well that this is perhaps the most intrusive investigative device which Parliament has authorized. When it was enacted, it was recognized that Part IV.1 gave the police expanded powers of investigation which, however, placed a substantial responsibility on the law enforcement agencies to comply fully. As a result, specialists have arisen within the police and prosecution to prepare the applications and carry out the authorizations, and it is not unreasonable to expect a high level of compliance. The often heard criticism of the exclusionary rule, namely, that it punishes the "cop on the beat" who is required to act quickly in emergency situations and who may not have the necessary training in the law, simply does not apply in this context.

209. Law Reform Commission of Canada, *Questioning Suspects*, [Report 23] (Ottawa: Minister of Supply and Services Canada, 1984).

210. Law Reform Commission of Canada, *Investigative Tests: Alcohol, Drugs and Driving Offences*, [Report 21)] (Ottawa: Minister of Supply and Services Canada, 1983).

Finally, the essence of the procedure for legalized wiretapping requires invocation of the court's process and justifies the court's taking a significant role in monitoring compliance through the only meaningful tool available, control over the trial process and admissibility of evidence. Seen in this context, even the absolute exclusionary rule is not much different from the modified "bring the administration of justice into disrepute" rule proposed in the other Commission Reports, since it is virtually implicit that failure to comply with a court order has an element of disrespect for the administration of justice.

(2) The Problem of Exclusion Generally

Under this heading we deal with the admissibility of evidence. Certain special rules have already been dealt with because of the important and specific policy considerations unique to those areas, namely, foreign interceptions (Recommendations 11 to 13) and interception of other offences (Recommendations 55 and 56).

Here, we deal more specifically with the problem of exclusion of evidence as the primary mechanism for enforcement of the legislative scheme. While in this discussion we deal briefly with the exclusionary rule generally, as it is formulated in current section 178.16 of the *Criminal Code*, the real problem dealt with is the impact of a review procedure. To focus the debate, we have set out two alternatives to the definition of substantive defect in the application. It will be recalled that we recommend exclusion of evidence as the remedy for a substantive defect in the application. The two alternative formulations delineate the parameters of the exclusionary rule in the review context. Those alternatives which can be described as "A": the rule of absolute exclusion, and "B": the good-faith exception rule, are as follows:

Alternative "A": Absolute Exclusion

That a substantive defect in the application means:

(a) none of the prerequisites set out in paragraph 178.13(1)(*b*) existed; or

(b) reasonable and probable grounds did not exist to believe that a targeted offence was being committed by a person provided for in the authorization; or

(c) any other grounds from which it may reasonably be concluded that, had the true state of affairs been known, the authorization would not have been granted, or not granted in substantially the form in which it was granted.

Alternative "B": Good-Faith Exception

That a substantive defect in the application means that by reason of statements in the application or affidavit which to the knowledge of the investigators were false, or statements which were made recklessly without regard to their truth or falsity, or deliberate or reckless omissions, it is demonstrated that:

(a) none of the prerequisites set out in paragraph 178.13(1)(*b*) existed; or

(b) reasonable and probable grounds did not exist to believe that a targeted offence was being committed by a person provided for in the authorization; or

(c) any other grounds from which it may reasonably be concluded that, had the true state of affairs been known, the authorization would not have been granted, or not granted in substantially the form in which it was granted.

To focus the issues further, we include a discussion of the recent decision of the United States Supreme Court in *United States* v. *Leon*,[211] where that court for the first time recognized a good-faith exception to the Fourth Amendment exclusionary rule in circumstances of great relevancy to this Paper — namely, good-faith reliance on a judicial warrant. We then explore the rationale for an exclusionary rule, and conclude with our recommendations in this area. Let it be said that these are difficult policy choices and we favour that remedy which best balances the competing interests. The decision in *Leon* is an attempt at striking such a balance in the American context. Subsection 24(2) of the Charter is also an attempt to strike an appropriate balance in the context of the violation of constitutional protections. As will be seen, in the end we recommend very little change to the present exclusionary rule in Part IV.1; most of our recommendations are aimed at clarifying the procedure and the rules.

At present under Part IV.1 of the *Criminal Code*, the exclusionary rule operates in several respects:

(a) where there has been inadequate notice *per* subsection 178.16(4);

(b) where there is no authorization and no consent, that is, an unlawful interception;

(c) where there is an authorization, but the interception is not made in compliance therewith, that is, of a person's communication not provided for in the authorization;

(d) where the authorization is, in effect, reviewed and set aside.

These all apply to primary evidence, that is, the actual communication; a different test applies to derivative evidence.

Our recommendations would alter situations (a) (notice) but we do not propose any change in (b) (unlawful interception and no consent), and (c) (noncompliance with authorization). Since we propose a change in the sanctions for notice, a discussion is set out below. We should, however, briefly discuss at this point an issue concerning compliance with the authorization. Prior to the decision of the Supreme Court of Canada in *Lyons* v. *The Queen*[212] there was some uncertainty as to the scope of the prerequisite for admissibility in paragraph 178.16(1)(*a*) that the "interception" be "lawfully made." the majority judgment in *Lyons* deals with this problem in a wholly satisfactory way which respects both the principles of privacy and effective law enforcement.

In *Lyons*, Estey J. for the majority held that the process of interception is a single undertaking carried out under an authorization which cannot be segmented into legally

211. *United States* v. *Leon*, 104 S.Ct. 3405 (1984).

212. *Supra*, note 123.

consequential and inconsequential steps. Thus, for example, an unlawful act in the installation of the device could taint the legality of the interception. The Ontario Court of Appeal had come to a similar conclusion in two recent cases: *R.* v. *Papalia*[213] and *R.* v. *McCafferty*.[214] It was also held, however, that "lawfully made" in paragraph 178.16(1)(*a*) does not mean in compliance with all laws, but rather in compliance with Part IV.1. Thus, surreptitious entry for installation of a device, if done to implement the authorization, would be lawful. If done, however, before the authorization was granted, perhaps under cover of a search warrant (as in *McCafferty*), then the interception would not have been done pursuant to an authorization and would not have been lawfully made, even if no actual recordings were done until after the authorization was obtained.

C. Notice under Subsection 178.16(4)

The present provisions of Part IV.1, specifically subsection 178.16(4), require that the prosecution give the accused notice that it intends to adduce a private communication. The notice must be "reasonable" in time and contain a statement as to the time, place and date of the private communication. As well, a transcript must be provided if the tape recording is to be played; otherwise, a statement setting forth full particulars is required. In the absence of any of this material, the evidence is inadmissible. The notice provision, by its terms, applies to a lawfully intercepted private communication which seems only to refer back to the alternative in paragraph 178.16(1)(*a*), namely, evidence of private communications being admissible where the interception was lawfully made, rather than to paragraph 178.16(1)(*b*), which permits admission of evidence no matter how obtained with consent of one of the parties to the communication, not necessarily the accused. The notice requirements of subsection 178.16(4) essentially perform a discovery function and only a tenuous privacy function. In our view, the discovery function applies whether the evidence is adduced under either paragraph 178.16(1)(*a*) or (*b*). To date, however, case-law has held that notice is not required where the evidence is adduced with the consent of one of the parties.[215] In our view, there is no adequate rationale for this distinction. On the other hand, the scheme of the legislation is that the penalty for defective notice is exclusion of evidence. This seems a drastic sanction for provisions designed to serve primarily a discovery function. In our view, exclusion of evidence should be reserved for serious breaches of the provisions; the primary control mechanism in this area should be towards enforcing compliance. If the failure to comply with the notice provisions results in unreasonable delay, sanctions are available under the *Canadian Charter of Rights and Freedoms*.[216]

213. *R.* v. *Papalia* (1984), 13 C.C.C. (3d) 449 (Ont. C.A.).

214. *Supra*, note 147.

215. See: *R.* v. *Banas and Haverkamp* (1982), 65 C.C.C. (2d) 224 (Ont. C.A.); *R.* v. *McDonald and Tondu* (1981), 60 C.C.C. (2d) 336 (Alta. C.A.).

216. Particularly the guarantee to a trial within a reasonable time in paragraph 11(*b*).

Of course, as set out above, the notice requirements would be extended to require the Crown to provide a copy of the authorization or renewal and the material referred to in section 178.14 which has not been ordered withheld by a court. The same reasoning applies, however, as failure to comply would not lead to exclusion of evidence, but only to sanctions designed to enforce compliance.

In the past, some question has arisen as to the application of section 178.16 to bail hearings. In a recent decision, *R.* v. *Kevork*,[217] Ewaschuk J. was of the view that the wording of paragraph 457.3(1)(*e*), which permits the justice to dispense with the strict pre-conditions as to admissibility of evidence, meant that section 178.16 did not apply at bail hearings. Whether or not this is a correct interpretation of sections 457.3 and 178.16, we are of the view that evidence of intercepted private communications or evidence derived therefrom ought to be admissible at bail hearings without a strict inquiry into the lawfulness of the interception, provided it was apparently made under an authorization or with the consent of a party. In this respect we note the proposed amendment to subsection 457.3(1) of the *Code* in subsection 85(1) of Bill C-18 (as passed by the House of Commons on April 24, 1985) which will add a new paragraph (*d*.1) as follows:

> the justice may receive evidence obtained as a result of an interception of a private communication under and within the meaning of Part IV.1, in writing, orally or in the form of a recording and, for the purposes of this section, subsection 178.16(4) does not apply to such evidence; ....

However, the wording of this amendment might be improved by making it clear that it was intended to cover both the communication itself and derivative evidence.

D. Substantive Defect in the Application

The real policy problem presented with respect to admissibility of evidence concerns the problem of review of the application for the authorization.

Simply put, the dilemma is this: What is the justification for excluding evidence where the evidence has been gathered by the police acting under, and in accordance with, a judicial mandate? If the point of the legislative scheme is to require judicial scrutiny prior to the interception, what are the compelling reasons for excluding evidence where a judge has passed on the merits of the application and, in the exercise of a judicial function, has authorized the intrusion? There is, of course, one clear case where the protection envisaged by the legislative scheme is subverted by the police conduct. This is the situation covered by alternative "B." The authorizing judge is really not in a position to assess properly the merits of the application and thus protect against

217. *R.* v. *Kevork* (1984), 12 C.C.C. (3d) 339 (Ont. H.C.J.).

unwarranted intrusion if he has been misled, intentionally or recklessly, as to the true state of affairs. In such circumstances, as in the *Gill* case,[218] the need for exclusion of evidence to deter such conduct is clear.

The more difficult case is where the authorities have made a proper application, relied upon the judge's determination that it is sufficient, acted in good-faith reliance upon the authorization only to find the evidence excluded because another judge determines that, for example, the material did not disclose the requisite reasonable and probable grounds.

The distinction between the two cases was considered by the Supreme Court of the United States in *United States* v. *Leon*,[219] where White J. speaking for the majority of the court carved out a good-faith exception to the rule of absolute exclusion of evidence obtained in violation of Fourth Amendment rights. The majority accepted that the requisite probable cause did not exist to issue a search warrant but held that evidence received pursuant to that warrant was nevertheless admissible. White J. considered that the rationale of the exclusionary rule was future deterrence of wrongdoing by the police, and that the rationale was not sufficiently strong in the case of good-faith reliance on a warrant.

Justice White considered at some length the rationale for the exclusionary rule, in particular with the concept of deterrence, and concluded that "[i]f exclusion of evidence obtained pursuant to a subsequently invalidated warrant is to have any deterrent effect, therefore, it must alter the behavior, of individual law enforcement officers or the policies of their departments," and further, "that suppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in these unusual cases in which exclusion will further the purposes of the exclusionary rule."[220]

The protection offered to privacy rights by Part IV.1 of the *Criminal Code* is similar to the protection offered by the Fourth Amendment (and its Canadian equivalent, section 8 of the *Canadian Charter of Rights and Freedoms*). The United States Supreme Court has determined that exclusion of evidence is not the appropriate remedy to protect those constitutional rights in certain circumstances when balancing the costs (essentially, acquitting the guilty) against the benefits (deterrence of future violations of the Fourth Amendment). What then are the arguments against the good-faith exception?

As might be expected, there was a vigorous dissent by Mr. Justice Brennan (Marshall J. concurring). He had foreseen this development in the shift in the courts' approach to Fourth Amendment issues over the previous ten years. Moreover, a debate has raged in the literature for at least that period over a good-faith exception, fueled most recently by the decision in *United States* v. *Williams*[221] where the United States Court of Appeal from the Fifth Circuit sitting *en banc* carved out a wide good-faith exception.

218. *Supra*, note 116.

219. *Supra*, note 211.

220. *Id.*, p. 3419.

221. *United States* v. *Williams*, 622 F.2d 830 (1980), cert. den. 449 U.S. 1127 (1981).

Justice Brennan in his dissent takes a much broader view of the purpose of the exclusionary rule. He does not see it as resting principally on a deterrence theory.[222]

Justice Brennan rejects the narrow deterrence theory, moreover, because of the impossibility of proof one way or another. As he says, quoting Justice Stewart in *Faretta* v. *California*,[223] "[p]ersonal liberties are not rooted in the law of averages."[224] On the other hand, he minimizes the costs of the exclusionary rule, pointing out that the evidence outside that subject to exclusion by reason of Fourth Amendment violation, would likely be sufficient to lead to a conviction.[225] Justice Brennan does, however, support an institutional deterrence theory which proposes that the demonstration "that our society attaches serious consequences to violation of constitutional rights is thought to encourage those who formulate law enforcement policies, and the officers who implement them, to incorporate Fourth Amendment ideals into their value system."[226]

Dealing specifically with the warrant question, Justice Brennan sees dangers in the good-faith doctrine in that there may well be a decreasing incentive for both police and magistrates carefully to prepare and consider applications.

Justice Stevens in his dissent focuses on the purposes of the Fourth Amendment and on an aspect of the debate seemingly overlooked; that is, that the historical roots of the Fourth Amendment are in the abuse of the warrant procedure and the desire of the framers of the Constitution to protect against general warrants and writs of assistance. Historically, "the paradigm of an abusive search was the execution of a warrant not based on probable cause."[227] He sees the exclusionary rule as designed to prevent violation of the Fourth Amendment and the good-faith exception as doing "grave damage to that deterrent function."[228] He also expresses concern over the concept of the courts relinquishing responsibility for constitutional violations.

Thus, we have the two sides of the debate presented in what may be a pivotal constitutional case in the United States where there has been experience with an absolute exclusionary rule for almost twenty-five years in state prosecutions[229] and almost seventy years in federal prosecutions.[230] It is apparent that an examination of that experience should prove useful in the attempt to determine the appropriate rule in the Canadian wiretap context. While it must be borne in mind that the debate in the United States is in a constitutional context involving the enforcement of a constitutional guarantee, this does not necessarily diminish its relevance. Privacy, whether a right of constitutional

222. *Supra*, note 211, pp. 3436-7.

223. *Faretta* v. *California*, 422 U.S. 806 (1975).

224. *Id.*, p. 834.

225. *Supra*, note 211, p. 3439.

226. *Id.*, p. 3443.

227. *Id.*, p. 3453.

228. *Id.*, p. 3454.

229. Since *Mapp* v. *Ohio*, 367 U.S. 643 (1961).

230. Since *Weeks* v. *United States*, 232 U.S. 383 (1914).

dimension in law, is certainly increasingly perceived as an important, if not fundamental, right in a modern society. Respect for privacy and restraint on intrusion into legitimate privacy interests underlie much of the work in the Police Powers Project, particularly when considering the reach of such an intrusive device as electronic surveillance.

To start with, then, what is the foundation for an exclusionary rule?

(a) *It is mandated by the Constitution.* This theory developed in the United States on the basis that use of documents seized in violation of the Fourth Amendment would violate the Fifth Amendment guarantee against self-incrimination.[231] This is not a theory which is now generally accepted.[232] It is, however, a theory which has some impact in the Canadian context where our *Canadian Charter of Rights and Freedoms* contains an explicit, if limited, rule of exclusion in subsection 24(2). On this theory, exclusion of wiretap evidence would be justified *if* the accused's constitutional rights were violated *and* the test in subsection 24(2) were met. Certainly, good faith on the part of the authorities is an important consideration in the "all the circumstances" equation.[233]

Any wider or different exclusionary rule must therefore rest on different foundations. It is necessary to explore these for two reasons: first, it is not clear what violations of the statutory wiretap regime are of constitutional impact and it is even less clear when admissions of evidence would bring the administration of justice into disrepute; second, constitutional violations can be expected to take care of themselves. No special legislative mechanisms are required. While it must be borne in mind that even for constitutional violations, Parliament has adopted a far more diluted test than one of absolute exclusion, this does not prevent the adoption of the same or a different rule if its adoption can be justified on another basis.

(b) *Exclusion to preserve the integrity of the government and the courts.* Under this theory, exclusion is required to prevent the government from receiving the aid of the judiciary in giving effect to a Fourth Amendment violation and to prevent the court from committing a second Fourth Amendment violation. Again, while this is not a theory given much credence in the United States,[234] it has relevance to the Canadian debate and in fact answers some of the exclusion problems. In the wiretap context, the issue can be reformulated as follows: Would the court, by admitting the evidence, be party to the commission of a criminal offence? This was a motivating force behind the exclusion of evidence in the case of *R.* v. *Stewart*,[235] even though on its face the regulation did not call for exclusion. Although the normal rule in Canada is that illegally obtained evidence is admissible, that

231. *Supra*, note 229.

232. Potter Stewart, "The Road to *Mapp* v. *Ohio* and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases" (1983), 83 *Colum. L. Rev.* 1365, p. 1381.

233. See: *R.* v. *Simmons*, *supra*, note 86; *R.* v. *Rao*, *supra*, note 46.

234. *Supra*, note 232, pp. 1382-3.

235. *R.* v. *Stewart* (1981), 60 C.C.C. (2d) 407 (Ont. C.A.).

rule does not touch the situation where "the very use or disclosure of the evidence in the course of the trial was unlawful"[236] in which case Parliament's intent must have been exclusion of the evidence.

Admittedly there is a certain artificiality to this foundation in the law reform context since it would be open to the reformers to distort the exclusionary rule by redefining the offences. However, with this borne in mind, what aspects of the regime does this basis for an exclusionary rule encompass? For our purpose, this requires an examination of the exception from liability by subsection 178.2(2) for the disclosure offence created by subsection 178.2(1):

> (2) 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 he may be required to give evidence on oath where the private communication is admissible as evidence under section 178.16 or would be admissible under that section if it applied in respect of the proceedings;
>
> (*b*) in the course of or for the purpose of any criminal investigation if the private communication was lawfully intercepted; ....

This then relates back to paragraph 178.16(1)(*a*) and the requirement that the interception was lawfully made, which in turn leads to section 178.11 which gives the parameters of lawful interception. For the purposes of this discussion, that involves two situations: consent interceptions (paragraph 178.11(2)(*a*)), and authorized interceptions (paragraph 178.11(2)(*b*)). It is the latter which is most important; it provides that the interception offence is not committed by:

> ... a person who intercepts a private communication in accordance with an authorization or any person who in good faith aids in any way a person whom he has reasonable and probable grounds to believe is acting with any such authorization; ....

Thus, exclusion of evidence is mandated to avoid the commission of an offence where the interception was not made in accordance with the terms of an authorization. This is the present Canadian position[237] which we do not propose to change. Rather, as indicated *supra*, this rule will remain. It should be noticed that good-faith interception in accordance with the authorization does not exempt from liability the interceptors, only persons, such as telephone company employees, who assist the interceptors in the interception. Accordingly, there is no room for a good-faith exception to the "in accordance with the terms of the authorization" admissibility requirement.

On the other hand, this analysis does not really answer the problem of review of the authorization. It would, of course, be possible to create the fiction that if there is

236. *Id.*, p. 437.

237. See: *R.* v. *Welsh and Iannuzzi (No. 6)*, *supra*, note 31; *R.* v. *Niles*, *supra*, note 163.

a substantive defect in the application, then the authorization is set aside,[238] so that in law, the officers were not acting in accordance with the terms of the authorization and therefore were acting illegally *per* subsection 178.11(1). However, this kind of retroactive imposition of liability is offensive to ordinary notions of justice even leaving aside nice questions of *mens rea* and the application of paragraph 11(*g*) of the *Canadian Charter of Rights and Freedoms*. A much more satisfactory approach is to address the review problem directly by acknowledging the fact that the authorities did intercept in accordance with an authorization, which at that time was valid, and to ask whether notwithstanding this fact and notwithstanding that they committed no offence in doing so and would commit none by the act of introducing the evidence obtained in court, there is some other basis for exclusion of evidence where there was a substantive defect in the authorization.

Under the theory of exclusion as a required remedy for enforcement of the scheme, exclusion of evidence is required in the Fourth Amendment context to ensure that the government does not violate the Fourth Amendment. It is justified then only if other adequate remedies of enforcement do not exist.[239] This then is the focus of the deterrence debate. Herein lies the justification for the good-faith exception. It is in this context that the rationale, if any, for exclusion of evidence on any basis is warranted for defects in (or violation of) the authorization application procedure. This requires examination of the costs and benefits of an exclusionary rule, and of alternative remedies.

It should be pointed out that, as in the Fourth Amendment exclusionary rule debate, there is one given — namely, it is a good thing for the authorities to comply with the statutory scheme (as it is a good thing for the authorities in the United States to comply with the Fourth Amendment). That one seeks remedies of any kind for violations of the scheme is part of the commitment to ensuring that it remains an effective protection against violations of the scheme and of legitimate privacy interests. Two questions must be asked:

1. What are the purposes of any remedy?

   (a) Specific deterrence: deterring the particular officer from repeating the same violation of the legislative scheme.

   (b) General deterrence: deterring other officers from repeating the same violation of the scheme.

   (c) Systemic deterrence: encouraging the authorities to put in place mechanisms to prevent future violations.

2. What are the alternative remedies to exclusion of evidence?

238. *Wilson* v. *The Queen*, *supra*, note 167.

239. *Supra*, note 232, p. 1384.

(1) Tort Remedy

One alternative to exclusion of evidence which would operate to secure compliance would be to put in place a statutory tort remedy, allowing the victim of an improperly authorized interception to sue the authorities. The American literature, however, almost uniformly admits its ineffectiveness in securing compliance.[240]

In our view, many of the same considerations would make a statutory tort remedy an ineffective means of securing compliance to the Part IV.1 process. Moreover, certainly to date, civil remedies have not been the preferred route either for remedying violations or for securing enforcement. Part I.1 of the *Crown Liability Act*,[241] and section 178.21 of the *Criminal Code* provide for damage awards for unlawful interceptions or disclosures either by agents of the Crown or private persons. We are unaware of any action (successful or otherwise) against any officer for any activity related to electronic surveillance, notwithstanding that, it is argued, when evidence is excluded under paragraph 178.16(1)(*a*), a possible tort action would lie.

(2) Criminal Liability

Another alternative to exclusion of evidence would be to widen the criminal liability by creating offences designed to ensure compliance with the application procedure. Again, experience would indicate that this is not an effective remedy for compliance.[242]

It is notoriously difficult to obtain convictions of police officers even in cases in which outrageous conduct is alleged. This is not to pass judgment on the validity or not of these allegations, but the institutional barriers including proof of *mens rea*, proof beyond a reasonable doubt and reliance on brother officers to provide evidence, all work against threat of criminal prosecution as a realistic enforcement mechanism. Once again, experience under Part IV.1 bears this out. Paragraph 178.22(3)(*a*) requires the annual report of the Attorney General or Solicitor General to set forth "... 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 178.11 or section 178.2; ...." We could find no report of any such prosecution. Further, we are unaware of the prosecution of any member of a municipal or provincial police force.[243]

240. William J. Mertens and Silas Wasserstrom, "The Good Faith Exception to the Exclusionary Rule: Deregulating the Police and Derailing the Law" (1981), 70 *Geo. L.J.* 365, pp. 406-10; Stewart, *supra*, note 232, pp. 1387-8; William A. Schroeder, "Deterring Fourth Amendment Violations: Alternatives to the Exclusionary Rule" (1981), 69 *Geo. L.J.* 1361, pp. 1386-96.

241. *Crown Liability Act*, R.S.C. 1970, c. C-38, as amended by S.C. 1973-74, c. 50, s. 4.

242. Schroeder, *supra*, note 240, pp. 1396-8; Stewart, *supra*, note 232, pp. 1386-7.

243. While we have recommended the creation of an offence for unauthorized surreptitious entry, we admit that this is to some extent symbolic but reflective of the seriousness with which we view this particular intrusion.

(3) Extrajudicial Controls

Under this heading might be considered independent review boards and internal disciplinary procedures. To the extent that their mechanisms would depend on initiation of action by citizens, they suffer from the same defects as the remedies considered above. While an independent review board could be founded on referrals by trial judges, it is unlikely that this would represent a sufficient enforcement mechanism. If the manner in which the application is made is legally irrelevant to the trial, then there would be no incentive to uncover violations of the application procedure. To the contrary, with the increasing pressure on the courts brought about by case-load and delays, there is a real disincentive on the part of the judge to embark on legally irrelevant lines of inquiry, and no particular incentive on the part of the accused or the Crown to make the inquiry. Internal controls suffer from many of the same disincentives. "Police officers often ignore serious misconduct by fellow officers and Courts rarely notify police administrators of misconduct by their officers."[244]

(4) Exclusionary Rule

This then leaves consideration of the exclusionary rule; however, only within a very narrow compass, namely, enforcement of compliance with the application procedure by exclusion of evidence in cases of substantial noncompliance. We have already set out the two alternative models, one based on automatic exclusion for failure to comply, and one based on exclusion only where there is not good-faith compliance. The costs of exclusion previously referred to include inaccurate fact-finding — normally resulting in: the guilty going free; otherwise meritorious charges being dropped or plea bargained for inadequate sentence; and, disrespect for the law as a result of the perception that the guilty are set free or inadequately dealt with.

A significant criticism of an exclusionary rule is that, like the other proposed remedies, it does not in fact deter misconduct.

First, let us give consideration to the costs. While many studies have been done in an attempt to quantify the costs in terms of lost or dropped prosecutions as a result of the Fourth Amendment exclusionary rule, the studies are probably inconclusive.[245] Advocates of the absolute exclusionary rule tend to minimize the costs.[246] Advocates of its abolition tend to magnify those costs. It has, however, been pointed out that the impact on serious cases such as murder is exaggerated and that in most instances other

244. Schroeder, *supra*, note 240, p. 1401. See also Stewart, *supra*, note 232, p. 1388.

245. See: Thomas Y. Davies, "A Hard Look at What We Know (and Still Need to Learn) about the Costs of the Exclusionary Rule: The NIJ Study and Other Studies of 'Lost' Arrests" (Summer, 1983), 3 *American Bar Foundation Research Journal* 611; Bradley C. Canon, "Ideology and Reality in the Debate over the Exclusionary Rule: A Conservative Argument for Its Retention" (1982), 23 *S. Tex. L.J.* 559; Mertens and Wasserstrom, *supra*, note 240; Schroeder, *supra*, note 240, pp. 1382-5.

246. Stewart, *supra*, note 232, p. 1394.

evidence is available.[247] This is not to minimize the seriousness of these costs but only to put them in focus.[248] Certainly, some of the recent case-law under the Charter have raised the same considerations.[249] Similarly, attempts to quantify the deterrent impact of the rule on police behaviour have been inconclusive.[250] Ultimately, this aspect of the debate must proceed on the basis of intuitive arguments.[251]

Some of these arguments may lose their force in the area of electronic surveillance applications because of the way these applications are prepared. These are not quick on-the-spot decisions, but rather the product of scrutiny at various levels, until passed on by a designated prosecutor with some expertise in the area. Thus, court decisions, for example, on what constitutes reasonable grounds or lack of alternative investigative means, would impact on subsequent applications, and prevent future improper applications. As well, judges hearing the applications would become aware of the decisions.

Moreover, none can doubt the reality of an exclusionary rule. Unlike criminal or civil sanctions, judges do exclude evidence and police do modify their procedures in response.[252]

Further, exclusion of evidence following a judicial hearing serves the interests of developing guidelines for the authorizing judge as to what in law constitutes compliance with the application conditions such as reasonable cause, lack of alternative investigative procedures, and so forth, so as to prevent future violations.[253]

Advocates of the good-faith exception to the exclusionary rule argue that most of these interests are served by a rule which allows for admission of evidence where the authorities have not acted wilfully or recklessly to avoid the strictures of the law, without the high cost which is exacted by an absolute exclusionary rule. In effect there is a certain balancing test. The rationale seems particularly strong when police have acted in good-faith reliance on a warrant (or authorization, in the wiretap context). Schroeder stated the following:

> Special problems involving the use of a good faith test arise when an officer seeks and obtains a search warrant. A search conducted *in accordance with the terms of the warrant* necessarily involves good faith, unless the police misrepresent facts to the magistrate in order to obtain the warrant. Nevertheless, the attorney preparing the affidavit and applying for the warrant or the magistrate issuing the warrant frequently makes errors that might

247. Mertens and Wasserstrom, *supra*, note 240, pp. 445-6.

248. See Schroeder, *supra*, note 240, p. 1384.

249. For example, *R.* v. *Collins* (1985), 5 C.C.C. (3d) 141 (B.C. C.A.).

250. See: Dallin H. Oaks, "Studying the Exclusionary Rule in Search and Seizure" (1970), 37 *U. Chi. L. Rev.* 665; Schroeder, *supra*, note 240, pp. 1378-82; Davies, *supra*, note 245, especially pp. 627-9.

251. See Schroeder, *supra*, note 240, p. 1384.

252. See Mertens and Wasserstrom, *supra*, note 240, pp. 400-1.

253. Advocates of the Fourth Amendment exclusionary rule consider this an important purpose of the rule. See: Mertens and Wasserstrom, *supra*, note 240, pp. 401-6; Wayne R. LaFave, *Search and Seizure* St. Paul, Minn.: West Publishing, 1978), vol. 1, 1984 Pocket Part at pp. 13-8; Stewart, *supra*, note 232, pp. 1400-1.

invalidate an entire search. When the police have dutifully applied to a judge or a magistrate for a search warrant, and have executed the warrant in strict conformity with its terms, exclusion of the evidence thus obtained can have no possible deterrent effect on future police conduct. Of course, exclusion of the evidence might improve the decisions of those magistrates who issue warrants pro forma or who lack the ability to evaluate intelligently the evidence before them. Even conscientious and well-trained magistrates occasionally make mistakes, however, and in such cases exclusion has absolutely no deterrent value. Thus, it makes sense to retain the exclusionary rule only for warrantless searches and those searches made on the authority of warrants based on perjured testimony or on evidence so scant that no reasonable magistrate could have believed it. This would encourage bona fide resort to warrants while also protecting individuals against abuse of warrant procedures.[254] [Emphasis added]

The debate, however, is not all one way on the good-faith exception, and arguments have been advanced to support the broader exclusionary rule.[255]

One problem that is mentioned is that of judge shopping; this could be considered a serious potential weakness of a good-faith rule of the type outlined in our alternative "B." The legitimacy of that alternative depends on the neutrality of the issuing judge to safeguard against improper applications. Judge shopping implies that the prosecutor is able to choose the judge who will determine the validity of the application for an authorization and that this is done because the judge is partial, "Crown/police oriented" or perhaps merely inexperienced and likely to be overwhelmed by the application and the expertise of the police and the designated agent. Thus, in case of an application of doubtful merit or of great importance, the risk of refusal is minimized. In its more positive aspect, a particular judge may be selected because of his expertise, to ensure that everything is in fact in order so as to minimize future difficulties. This would be important where there is a perception that the litigation stemming from the authorization will be particularly hard fought and the material closely scrutinized.

A disadvantage of the secrecy provisions is that, on the one hand, not only is it impossible really to quantify judge shopping, but on the other hand, that very secrecy encourages the perception that it goes on. Ultimately, however, and despite claims to the contrary, we believe that judge shopping rests only on speculation.[256] In its most negative sense it depends on bad faith on the part both of the agent and the judge and we would be loathe to reject a rule, otherwise meritorious, on the basis of this kind of speculation.

This, however, does not take away from the importance of the perception that judge shopping goes on. As we have said, that perception, always present in any *ex parte* proceeding, is reinforced when the proceedings are forever secret and where no record is kept of what occurs. We would not want our proposed regime threatened by

254. Schroeder, *supra*, note 240, pp. 1418-9.

255. See, for example, the dissent in: *Unites States* v. *Leon*, *supra*, note 211; Stewart, *supra*, note 232, p. 1403; Mertens and Wasserstrom, *supra*, note 240; LaFave, *supra*, note 253, pp. 11-5.

256. However, see Cohen, *supra*, note 97, pp. 140-3 and references therein, particularly the U.S. *Report of the National Commission for the Review of Federal and State Laws Relating to Wiretapping and Electronic Surveillance* (1976), pp. 73-4.

the *perception* that judge shopping can undermine its safeguards. Since we recommend that the material used on the application be eventually disclosed to the defence, this should relieve some of the concern. One suggestion that has been made to deal with the problem of this perception is to follow the approach taken in the United States by the Administrative Office of the United States Courts in the Wiretap Report[257] and publish the names of the judges and the number of orders they have granted. This suggestion has been put to persons with whom the Commission has consulted in the past and there has been little enthusiasm for it. Moreover, it is not clear whether this really serves the purposes of avoiding judge shopping.

We would prefer that the problem be dealt with directly, and would hope to see the implementation of administrative rules which put in place a formal rotation system. Under such a system the prosecutor must simply take the judge assigned to do authorizations. This is obviously a system which cannot operate effectively in a small jurisdiction, but in such a jurisdiction the options for judge shopping are simply minimal. We are also aware of systems in some of the larger districts for having a panel of designated judges; provided such judges do not come to feel that they are allied within the prosecution because of the frequency with which they deal with such applications, we feel that such a system, designed to encourage expertise among the authorizing judges, is not inconsistent with our recommendation. We do not, however, feel that it is necessary that this be a formal recommendation.

Then, accepting the criticism of Justice Stewart and the other commentators, but bearing in mind the levels of authority involved in a wiretap application, one may ask, Is the limited good-faith exception as outlined in alternative "B" not the appropriate compromise? Such a test would eliminate the worst abuses and the possibility of judicial inquiry will protect against some improper applications. Some case-law will develop to guide authorizing judges, since an inquiry into good faith requires some investigation of the appropriate standards. The problem that a good-faith exception may place a premium on ignorance can be dealt with by excluding from good faith, reckless failure to comply with the statutory conditions. On balance therefore, *in the area of review of the authorization for substantive defects in the application*, we favour a good-faith exception to exclusion of evidence as the primary enforcement mechanism.

E. Derivative Evidence

Derivative evidence is that evidence, other than the private communication itself, which is obtained as a result of the acquiring of the private communication. Presently, section 178.16 contains a limited exclusionary rule as follows:

> (1) A private communication that has been intercepted is inadmissible as evidence against the originator of the communication or the person intended by the originator to receive it unless

257. *Supra*, note 150.

(*a*) the interception was lawfully made; or

(*b*) the originator thereof or the person intended by the originator to receive it has expressly consented to the admission thereof;

but evidence obtained directly or indirectly as a result of information acquired by interception of a private communication is not inadmissible by reason only that the private communication is itself inadmissible as evidence.

(2) Notwithstanding subsection (1), the judge or magistrate presiding at any proceedings may refuse to admit evidence obtained directly or indirectly as a result of information acquired by interception of a private communication that is itself inadmissible as evidence where he is of the opinion that the admission thereof would bring the administration of justice into disrepute.

In section 178.16, the rule is broadly framed applying to evidence obtained directly or indirectly. Any derivative evidence rule can pose difficult problems such as the following:

(a) If the derivative evidence was obtained from two sources only one of which is tainted, is it excludable?

(b) Upon whom is the burden of showing what evidence is derivative?

(c) Should derivative evidence be subject to automatic exclusion?

(d) Does issuance of a renewal or new authorization break the chain of taintedness?

Some of these issues were considered by Borins Co.Ct.J., in *R.* v. *Samson (No. 6)*.[258] In that case, His Honour found that much of the Crown's case was obtained directly or indirectly from inadmissible primary evidence. He considered that the burden was on the Crown to demonstrate that its evidence was not derivative. Further, it did not matter that the evidence might have been obtained from other sources. The question is, How in fact was it obtained? Evidence obtained from mixed (tainted and untainted) sources was also derivative. Further, he found that evidence obtained pursuant to a subsequent authorization was derivative if the application for the subsequent authorization was based on unlawful interceptions. On the Crown appeal[259] these issues were not dealt with in view of the court's determination that the primary evidence was admissible.

In considering these issues, we can draw on two streams of American experience: firstly, the experience under Title III, specifically section 2515 which provides that "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, ... if the disclosure of that information would be in violation of this chapter" and secondly, the "fruit of the poisonous tree" doctrine in Fourth Amendment jurisprudence. As it happens, however, it was the intent of Congress that the "fruit of the poisonous tree" doctrine principles apply to derivative evidence questions under section 2515.[260] Generally speaking, the burden is on the accused to demonstrate on a preponderance of evidence that the prosecution's evidence is tainted by the

258. *Supra*, note 102.

259. *Supra*, note 58.

260. See "The Legislative History of Title III, Senate Report No. 1097," which is Appendix B in David Watt, *Law of Electronic Surveillance in Canada* (Toronto: Carswell, 1979), pp. 378-9.

illegal interception. However, tainted evidence can include interceptions obtained under an order which was itself obtained by use of tainted evidence, and if the original order was tainted, any extensions are automatically tainted.[261]

Difficult questions can arise in applying the so-called attenuation rules, developed under the Fourth Amendment. For example, where the existence of a witness is discovered from an unlawful interception, when is that witness' testimony tainted and therefore inadmissible,[262] and what material is the accused entitled to see in order to meet the burden of establishing the taint?[263]

The recent trend in United States Supreme Court decisions is to cut down the scope of the "fruit of the poisonous tree" doctrine in Fourth Amendment legislation. This, of course, has a direct impact on taint litigation under Title III. The court has done this by extending the attenuation rules. A recent statement of that rule in *Segura* v. *United States*,[264] provides that the evidence is not to be excluded if it is " 'so attenuated as to dissipate the taint.' "

In Canada there are two weak analogies to the poisonous tree doctrine. As is well known, physical evidence obtained as a result of an illegal confession is admissible — the so-called *St. Lawrence*[265] rule. As well, the no-substantial-wrong proviso in subparagraph 613(1)(*b*)(iii) of the *Criminal Code*, which permits dismissal of an appeal notwithstanding errors of law at trial, is a type of attenuation rule. Thus, there is really little Canadian experience to draw upon. In our view, the primary purpose of a derivative evidence rule in the wiretap regime must be to deter wilful failure to comply with the statutory procedures and safeguards. When the wiretap Bill was first introduced the police represented that the optimal use of wiretaps was to gather intelligence, that is, to gather other evidence of criminal activity, not necessarily to use the communications themselves. We would not want to encourage a system whereby unlawful interceptions are made by the police for intelligence-gathering purposes without fear that evidence derived therefrom would nevertheless be inadmissible. This would undermine all the lawful protections of the legislative scheme and bring the administration of justice into disrepute.

On the other hand, we are very concerned to avoid the complexities which seem to be the inevitable product of any derivative evidence rule. In our view, many of the complexities in the United States derive from the rule of automatic exclusion which flows from a finding of taint. For that reason, the courts strain to take the evidence outside the taint rule. If we could therefore give the courts a discretion to exclude evidence and couple it with some simple rules as to what is derivative, then some of these problems would, it is hoped, be avoided.

261. See *United States* v. *Giordano*, *supra*, note 171.

262. See *United States* v. *Ceccolini*, 435 U.S. 268 (1978).

263. See *Alderman* v. *United States*, 394 U.S. 165 (1969). Generally, for a detailed discussion of all of these issues in the electronic surveillance field, see Carr, *supra*, note 67, Chapter 6.04.

264. *Segura* v. *United States*, 104 S.Ct. 3380 (1984), *per* Burger C.J., p. 3386.

265. *R.* v. *St. Lawrence*, *supra*, note 79; *R.* v. *Wray*, *supra*, note 8.

F. The Length of Proceedings

Over the years, since the enactment of Part IV.1, concern has been expressed as to the length of proceedings on the *voir dire*. Electronic surveillance is a highly intrusive means of investigation which has necessitated strict controls. As a result, proof of compliance with those controls takes time. As well, the evidence is sometimes highly technical and the legal arguments complex. While we must be concerned with the efficiency of court proceedings, it is fundamental that efficiency not interfere with due process. While we have, we hope, rationalized the review procedure, we do not think that any genuine due process or privacy interests have been infringed. As is apparent, we have attempted to limit admissibility issues to substantive issues which go to the heart of the reasons for the controls.

Where the defence wishes to litigate all issues in a wiretap case, the evidence can include testimony as to installation of the device, monitoring the device, preparation of tapes and transcripts, continuity, voice identification, proof of designation of agents, and so on. Experience has shown that defence counsel will often waive proof of many of these matters when there is no useful purpose served in defence of their client. We have included certain recommendations in an attempt to streamline areas of inquiry and proof, which are usually noncontentious.

RECOMMENDATIONS

57. That the reasonable notice referred to in subsection 178.16(4) apply whenever the prosecution seeks to introduce an intercepted private communication.

58. That where the prosecution has failed to give reasonable notice, a justice presiding at a preliminary inquiry or the trial judge may adjourn the proceedings for the purpose of requiring the prosecution to give reasonable notice and take whatever other steps are required to ensure that reasonable notice is given prior to the proceedings, taking into consideration the right of the accused to a trial within a reasonable time.

59. That section 457.3 be amended by including paragraph (*d*.1) as follows:

the justice may receive evidence of an intercepted private communication or evidence obtained as a result of an interception of a private communication apparently made under and within the meaning of Part IV.1, in writing, orally or in the form of a recording and, for the purposes of this section, section 178.16 does not apply to such evidence.

60. That primary evidence obtained by electronic surveillance be inadmissible unless:

(a) the interception was lawfully made

(i) with the consent of a party to the intercepted communication,

(ii) in accordance with the terms of an authorization;

(b) a party to the intercepted communication consents to the admission.

61. That where a defect exists on the face of the authorization or renewal, the trial judge shall admit the primary evidence obtained in apparent compliance with such authorization or renewal unless officers acting in apparent compliance therewith could not reasonably have believed that the authorization or renewal was valid.

62. That, for the purposes of Recommendation 51, a substantive defect in the application means that by reason of statements in the application or affidavit which to the knowledge of the investigators were false, or statements which were made recklessly without regard to their truth or falsity, or deliberate or reckless omissions, it is demonstrated that:

(a) none of the prerequisites set out in paragraph 178.13(1)(*b*) existed;

(b) reasonable and probable grounds to believe that a targeted offence was being committed by a person provided for in the authorization did not exist;

(c) any other grounds exist from which it may reasonably be concluded that, had the true state of affairs been known, the authorization would not have been granted, or not granted in substantially the form in which it was granted.

63. That evidence which is derived from primary evidence which is inadmissible, is itself inadmissible where in the opinion of the court, having regard to all the circumstances, to admit such evidence would bring the administration of justice into disrepute.

64. That evidence is derived from primary evidence where it would not have been obtained but for the acquisition of the primary evidence. However, evidence is not derivative where:

(a) it is obtained pursuant to an otherwise valid authorization although such authorization was based on evidence obtained as a result of an invalid authorization;

(b) it is the testimony of a witness to the commission of an offence although the witness' identity was discovered as a result of inadmissible primary evidence.

65. That once primary evidence is determined to be inadmissible, Crown counsel shall stipulate what, if any, evidence is derivative therefrom and the reasons why any other evidence is not derivative. That for the purposes of determining the validity of such reasons, the prosecution or the accused may, with leave of the

court, call any witness for the purposes of cross-examination, and the accused with leave of the court may inspect any tapes or transcripts related to the investigation, whether or not he was a party to the communication.

66. That affidavit evidence be admissible and, in the absence of evidence to the contrary, be *prima facie* proof of:

(a) the times and places of the interception;

(b) the custody and continuity of the tape recordings;

(c) the manner of interception;

(d) service of notice.

67. That a copy of the authorization signed by a judge be admissible without proof of the authenticity of the signature.

68. That recital in the authorization as to the status of the designated agent be proof of such designation.

VI. Miscellaneous Recommendations

A. Annual Reports: Section 178.22

Section 178.22 of the *Criminal Code* requires the Solicitor General or provincial Attorney General to prepare essentially a statistical report. The Commission has previously studied the weakness of the section 178.22 report[266] and considered various recommendations designed to strengthen accountability in this area. We have also been told that the Department of Justice has certain recommendations which it wishes considered in this particular area. Unfortunately, their recommendations are not yet complete and it is difficult for us to assess the impact of our other recommendations designed to increase accountability.

While useful information can be obtained from review of statistics, we are hopeful that some of our recommendations concerning disclosure of material and notice will serve to make the entire process more open and accountable with a corresponding diminution in the need to rely on statistics. Accordingly, for the present, we have made no recommendation for amendments to section 178.22.

266. Savage, *supra*, note 44.

B. Notice under Section 178.23

The present legislation, section 178.23 of the *Criminal Code*, requires the minister on whose behalf the application for an authorization was made to give notice in writing to the person who was the object of the interception within a specified period. Thus, no notice is required to a person who was the object of a consent interception, that is, one not done by means of an authorization. It is the nature of a properly conducted interception, of course, that the persons targeted are never aware of the operation, particularly if charges are never laid. This illustrates the need for some form of post-interception notice.

Section 178.23 of the *Criminal Code* as presently interpreted requires that the person who was the object of the interception merely be told of that fact. As held in *Re Zaduk and The Queen*,[267] the person is entitled to no greater notification, such as the date or period of the interception, a copy of the authorization or access to the tape recordings. The American legislation requires a somewhat wider notice and gives a discretion to the court to give further discovery:

> S. 2518(8)
>
> (d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of —
>
> (i) the fact of the entry of the order or the application;
>
> (ii) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and
>
> (iii) the fact that during the period wire or oral communications were or were not intercepted.
>
> The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.[268]

Since its enactment, virtually all persons who have considered the question have expressed dissatisfaction with the present notice procedure. It has been observed that in one sense the object of the interception would be better off not getting the notice, since the notice provided is so inadequate as to be useless and merely engenders anxiety and frustration. In our view, the notice under section 178.23 must be meaningful in relation to the purposes for which it is required. This calls for the identification of those purposes.

267. *Supra*, note 189.

268. Title III, *supra*, note 67, section 2518(8).

The case-law has identified two purposes. In *R.* v. *Welsh and Iannuzzi (No. 6)*[269] and *Re Zaduk and The Queen*, [270] the purpose identified was that of political accountability. In *Zaduk*, Mr. Justice Lacourcière described this accountability as flowing from the ability of the public "to monitor, in a general way, the application and practical effect of the new legislation." It was his view that section 178.23 was not intended as a means of advancing a civil suit for improper interception. As His Lordship pointed out, civil liability flows from "unlawful, i.e. unauthorized, interceptions." Weatherston J.A., dissenting, came to the opposite conclusion. It was his view that some mechanism must be available for furthering the civil remedies that could flow from an unlawful interception. As His Lordship pointed out, the authorization may have permitted some means of interception at certain places and not others. Without more information, the targeted person is left without any way of determining whether the interceptions actually conducted were within the terms of the authorization. To quote Justice Weatherston: "A citizen is entitled to the protection of the law. How can he enjoy that protection unless he knows the extent to which his rights have been invaded?"[271]

The problem of adequate civil remedies for unlawful interception is beyond the scope of this Paper. We have, therefore, not specifically approached this problem from the point of view of civil discovery. On the other hand, we feel that the principles of reviewability and accountability which have guided the work in the police powers areas call for more than section 178.23 now requires. An appropriate analogy is where the police search unoccupied premises under a warrant. In Working Paper 30[272] it is recommended that a copy of the warrant should be suitably affixed within any place that is unoccupied at the time of the search. It is an important principle that intrusions into privacy be justifiable and justified. At a minimum, therefore, the apparent justification for the massive intrusion by electronic surveillance must be given to the person affected. He should, therefore, be entitled to know when the intrusion took place and under what authority. We are also of the view that some mechanism should be in place for a further disclosure in an appropriate case. We consider these proposals to be the minimum where no charges are laid against the target and he does not have the fuller disclosure or notice mandated by section 178.16.

A recent decision of Steele J., styled *R.* v. *X*,[273] has pointed out a problem with the drafting of subsection 178.23(4). This provision gives a judge power to extend the period during which notification may be given by up to three years, provided *inter alia* "the investigation of the offence to which the authorization relates is continuing." It may happen, as in the *X* case, that the first authorization will be in relation to certain offences but that the investigation may have ceased. In the meantime, investigation into other offences for which new authorizations were obtained may be continuing. However, the wording of subsection 178.23(4) would preclude the judge from extending the notice

269. *Supra*, note 31.

270. *Supra*, note 189, p. 332.

271. *Id.*, p. 341.

272. *Supra*, note 47, Recommendation 27, p. 350.

273. *R.* v. *X*, Ont. H.C.J., *per* Steele J., May 15, 1984 (unreported).

period on the first authorization. In our view, the need for an extension is legitimate in the latter case, since any notification would likely frustrate the ongoing related investigation. Accordingly, the statute should be amended to cure this problem.

A further problem concerns sanctions for failure to give the section 178.23 notice. Case-law has uniformly held that failure to give notice has no effect on the admissibility of evidence where charges, in fact, are laid as a result of the investigation.[274]

Only in exceptional circumstances can exclusion of evidence be justified on the basis of noncompliance with statutory provisions that do not go to the legality of the interception. At present, the *Protection of Privacy Regulations*[275] require that the Attorney General or Solicitor General certify to the court the manner in which the notice was given. In the case where the person is never charged, so that the section 178.16 notice provisions never apply, this is adequate, subject to a slight change in wording to reflect that the certification requirement arises not simply "where the notice was given by him" but from the fact that notice is required under section 178.23. We see no need for any particular sanction in the absence of some particular indication that the present regime is not adequate.

Where charges are laid *and* notice is served under section 178.16, we think that such notice is adequate and see no requirement for further notice under section 178.23, having regard to the purposes for which the latter notice is given. However, where charges are laid and the Crown does not intend to rely on wiretap evidence, the accused may never get a notice under section 178.16 and never learn of the interception, unless there is compliance with section 178.23. Knowledge of the interception may be important to the accused's ability to make full answer and defence. In the recent case of *R.* v. *McLeod*,[276] one of the accused on a charge of murder relied on the defence of alibi. He was a member of a motorcycle gang, and unknown to him the gang's clubhouse was wiretapped. It was only after the conviction on appeal and by purely fortuitous circumstances that his counsel learned that tapes existed of his conversation the night of the killing, which tended to support the alibi. As a result, his conviction was set aside and a new trial ordered based on this fresh evidence.

Further, so long as there is even a limited exclusionary rule, it is important that the accused be aware of the existence of any interceptions. Some mechanism must be in place such as section 178.23 to provide him with that notice.

Finally, we have given some consideration to whether there should be notice in cases of consent interceptions. However, since the reason for post-interception notice really arises from the fact that none of the parties are aware of the interception, we do not believe the same policy considerations require notice in those cases. We would

274. *R.* v. *Welsh and Iannuzzi (No. 6), supra*, note 31; *R.* v. *Miller and Thomas (No. 4)* (1975), 28 C.C.C. (2d) 128 (B.C. Co.Ct.).

275. *Protection of Privacy Regulations*, C.R.C. 1978, vol. 5, c. 440.

276. *R.* v. *McLeod*, Ont. C.A., April 13, 1982 (unreported).

also be concerned about possible danger to informers and other police operatives who, perhaps at some risk to themselves, had agreed to be bodypacked. On balance we see no need for notice outside the trial process in such circumstances.

After the project has concluded and the time comes to give notice, it may be that the person is no longer traceable. It is the policy of some police forces to serve the section 178.23 notice personally, even though the legislation does not require this, and to file an affidavit with the court when the party cannot be located. We feel that the affidavit procedure is a good one, although we consider that a signed statement by the officer is sufficient.

RECOMMENDATIONS

69. That where notice under subsection 178.16(4) has not been given, a person who was the object of an interception shall be given notice of the dates of the interceptions and a copy of the authorization under which the interception took place.

70. That, upon written application by the accused, a judge with power to grant an authorization, or the trial judge, may require the prosecution to disclose such details of interceptions as may be necessary for an accused to make full answer and defence.

71. That, for the purposes of Recommendation 65, the judge may require the prosecutor to make such inquiries of law enforcement agencies as the judge considers necessary.

72. That notice under section 178.23 shall be given within ninety days of the termination of the authorization or renewal or such greater period not exceeding three years, where a judge is satisfied that by reason of a continuing investigation the giving of notice within ninety days would be contrary to the interests of justice.

73. That where notice cannot be given under section 178.23 because the person cannot be located, a peace officer with knowledge of efforts made to locate the person shall submit a statement in writing to the court setting out the reasons why notice has not been given and efforts made to locate the person.

C. The Disclosure of Intercepted Private Communications

Section 178.2 of the *Criminal Code* enacts a prohibitory and preventive scheme which regulates the use and disclosure of intercepted private communications, in whole

or in part, or the substance, meaning, purport or existence of such whole or part, absent consent by a party to the interception, use or disclosure.[277]

The listed exceptions of subsection 178.2(2) exempt from the prohibition of the preceding subsection such use or disclosure as is made for investigative, evidentiary or service purposes. We see no reason to disagree with the rationale underlying such exemptions which represent, as we view it, a proper balance of privacy, law enforcement and fair trial considerations. There are, however, practical considerations which, consistent with the aforementioned *rationalia*, argue most persuasively in favour of at least a clarification if not expansion of the listed exceptions in subsection 178.2(2).

Investigations involving electronic surveillance characteristically produce hundreds if not thousands of hours of monitoring, corresponding transcripts of recorded communications, and seemingly endless interception logs. Significant evidentiary problems routinely emerge in such cases and, not infrequently, experienced prosecutorial assistance is sought to determine whether or what proceedings may be instituted. Indeed, independent prosecutorial review of the fruits of the interception process at such an early stage is highly desirable to ensure that only legally sufficient cases engage the attention of the criminal process. The present investigative disclosure exceptions, paragraphs 178.2(*b*) and (*e*), while arguably of sufficient breadth to permit the disclosure here considered, in our view, ought to be expanded so as to permit it expressly. The proposed expansion does not, in our view, compromise any recognizable privacy interest nor otherwise impair the spirit of the recommendations here made.

Private communications intercepted in accordance with an authorization granted by a competent Canadian judicial authority, on occasion, may afford evidence of crimes committed entirely beyond our borders or of offences about to take place there. There exists some divergence of opinion as to whether information obtained through judicially authorized Canadian interceptions can be lawfully transmitted to foreign law enforcement agencies. While it seems highly desirable that such information be made available to the appropriate authorities in foreign jurisdictions, if for no reason than to be consonant with some of our international obligations, it is of equivalent significance that such disclosure should only be to properly authorize investigative or law enforcement officers in limited circumstances. To put the matter somewhat differently, such disclosure ought to be permissible only when made to investigative or law enforcement officers in the foreign jurisdiction and to the extent that it reveals a past, current or potential crime in such jurisdiction.

RECOMMENDATION

74. That subsection 178.2(2) be amended expressly to exempt from the prohibition of subsection 178.2(1) the following:

(a) where the disclosure is made to a peace officer, the *Attorney General or his agent* and is intended to be in the interests of justice; and,

277. *Criminal Code*, s. 178.2(1).

(b) where the disclosure is made to an investigative or law enforcement officer in a foreign jurisdiction and tends to reveal a past, ongoing or prospective crime in such jurisdiction.

D. Assistance in the Execution of Orders

Intractable difficulties have arisen in the execution of judicial authorizations where assistance is required from persons in charge of premises in respect of which interceptions are to take place and organizations engaged in providing telephone, telegraph or other communications services. It has been found, for example, particularly in the provinces of Ontario and Québec, that interceptions authorized by judicial order cannot be carried out because the necessary information and assistance have not been furnished by the relevant communications company. The fact and extent of the invasion of privacy have been judicially determined, but the lack of assistance at least delays the execution of the order and, on occasion, entirely frustrates it.

Analogous arguments have earlier been rehearsed in connection with surreptitious entry. By parity of reasoning, we can see no justification for permitting explicit authority to be given to enter premises to install interception devices for the purpose of giving effect to an authorization, but withholding it where assistance falling short of an actual invasion of the target's property only is required. We would make two further observations. To include a statutory requirement of furnishing assistance as is done in section 2518(4) of Title III should also carry with it both an appropriate penalty for noncompliance and an exemption from interceptional liability under subsection 178.11(2). Secondly, the communication's organization ought to be compensated for its assistance at the prevailing rates for the service provided.

RECOMMENDATIONS

75. That the authorizing judge be given express authority to order any person, including companies and organizations, engaged in providing communication or telecommunication services, as well as landlords, custodians or persons in charge of premises, to furnish all such technical or material assistance or information as may reasonably be required to accomplish the interception in accordance with the authorization, and to be compensated therefor at the prevailing rates.

76. That failure of compliance in accordance with the authorization shall be punishable as contempt of court.[278]

278. See, for example, subsection 533(2) of the *Code*, which makes failure to comply with the terms of an order releasing exhibits for scientific or other testing or examination punishable as contempt.

CHAPTER FOUR

Summary of Recommendations

The Offence

1. That the offences for which an authorization would be available continue to be listed. That the following offences be omitted from the present list in section 178.1: *Criminal Code* ss. 58 (forgery, etc.), 159 (obscene material), 195(1)(*a*) (procuring), 281.1 (advocating genocide), 314 (theft from mail), 331 (threatening letters, etc.), 339 (using mails to defraud); and *Excise Act*: ss. 158 and 163 (unlawful distillation or selling of spirits).

2. That the following *Criminal Code* offences be added to the list: ss. 195(1)(*b*), (*c*), (*d*), (*h*) and (*i*) (procuring, etc.), 305.1 (criminal interest rate), 381.1 (threats to commit offences against internationally protected person).

3. That the organized crime definition for offences be omitted but an authorization be available for investigation of: a conspiracy to commit; attempt to commit; being an accessory after the fact; and counselling, procuring or inciting in relation to any of the listed offences.

Private Communications

4. That "private communications" be defined as follows:

> **any oral communication or any telecommunication made under circumstances in which it is reasonable for any party to it to expect that it will not be intercepted by any electromagnetic, acoustic, mechanical or other device.**

5. That a communication does not cease to be a private communication only by reason of a belief on the part of a party to it that the communication may be the subject of an authorization obtained from a court by a law enforcement agency.

6. That subsection 178.11(2) be amended by the addition of paragraph (*e*) as follows:

a person engaged in monitoring for security purposes of communications of inmates of a prison as defined by the *Prisons and Reformatories Act*, R.S.C. 1970, c. P-21, and a penitentiary as defined by the *Penitentiary Act*, R.S.C. 1970, c. P-6, where the fact that such monitoring may occur is prominently displayed at the place where the communication may occur.

7. That the definition of "electromagnetic, acoustic, mechanical or other device" be amended as follows:

"electromagnetic, acoustic, mechanical or other device" means any device or apparatus that is used, or is capable of being used, to intercept a private communication, but does not include a hearing-aid used to correct subnormal hearing of the user to not better than normal hearing, nor a device such as a pen register, touch-tone decoder, diode device or other similar device used to acquire the identity of the telephone number dialed, or of the caller, the time and the date of the telephone call, but which is not capable of intercepting any words or other information.

Optical Devices

8. That it be an offence to enter private property without a court order or the consent of the owner or lawful occupier for the purpose of installing an optical device.

9. That an authorization to install an optical device be available by application to a court, but only under the same conditions as an authorization is available for installation, by surreptitious entry, of a listening device.

10. That "optical device" be defined for the present time as any electronic device or mechanism capable of permitting surreptitious viewing of persons or things.

Foreign Interceptions

11. That primary and derivative evidence obtained from an interception made outside Canada, no matter where the private communication originated, be admissible in evidence whether or not the interception was lawfully made, provided that the interception was not made in the foreign jurisdiction in violation of the laws of the jurisdiction with the connivance of Canadian authorities.

12. That the court before which evidence from a foreign interception is tendered shall conduct an inquiry into the admissibility of that evidence only where

the person against whom the evidence is sought to be admitted leads some evidence from which the court could find that the interception was made in violation of the laws of the foreign jurisdiction with the connivance of Canadian authorities.

13. That the notice provisions in present *Code* subsection 178.16(4) apply to evidence obtained from foreign interceptions.

Participant Monitoring: Consent Interceptions

14. That section 178.11 continue to provide that it is not unlawful to intercept private communications where the interception is made with the consent, express or implied, of any party to it.

15. That the offence in subsection 178.18(1) not apply to any person in possession of a device or component for the purpose of using it in an interception made or to be made with the consent of one of the parties.

16. (1) That a peace officer, before commencing an interception under this section, shall inform the person whose consent is sought that he has a right to refuse to consent and to withdraw his consent at any time.

(2) That consent under this section may be given orally or in writing.

17. That the signature of a person on a document warning him of his right to refuse to consent and of his right to withdraw his consent at any time or a recording of such consent be *prima facie* proof of the consent of the person to the interception.

The Application Procedure

18. That the application for an authorization or renewal continue to be in writing and accompanied by an affidavit of a peace officer. The hearing shall be *ex parte* and *in camera*. The judge should be empowered to place the peace officer under oath to ascertain additional facts underlying the application. However, if such facts are relied upon in the adjudication of the application, a record of such facts shall be included in the sealed packet.

Basis for Granting the Authorization

19. That paragraph 178.13(1)(*a*) be amended to provide that the judge may grant an authorization where he is satisfied that it would be in the best interest of the administration of justice and in the public interest having regard to the seriousness of the offence under investigation.

Interprovincial Offences

20. That subsection 178.12(1) be amended to provide that an authorization may be granted where the communications of the targeted person may be intercepted in one province, although the offence is alleged to have been committed in another province.

Minimization

21. That an authorization may only be granted in relation to persons the interception of whose private communications will assist in the investigation of the offence by reason of their involvement in the offence.

22. That section 178.13 be amended to provide that the judge, in granting the application, may include any of the following terms and conditions:

(a) that the device be live monitored at all times that it is proposed to intercept or record private communications;

(b) that so far as is reasonably possible, only the conversations of targeted persons be intercepted and recorded;

(c) that where it is proposed to intercept communications at a telephone to which the public has a right of access, then any interceptions shall be on the basis of live monitoring and accompanied by visual surveillance;

(d) that reasonable steps be taken not to intercept private communications between spouses, physician and patient or persons in other confidential relationships;

(e) that reasonable steps be taken not to intercept private communications of targeted persons which by reason of a known pattern are unlikely to assist in the investigation of the offence;

(f) that interception cease after the object of the investigation has been obtained;

(g) that, where the interception of a telephone line will involve a party line, no interception occur except when the line is being monitored;

(h) such further terms and conditions as the judge considers advisable to minimize the acquiring and recording of private communications which would not assist in the investigation.

23. That the authorization shall include a term requiring that, where an interception is to occur at a place mentioned in subsection 178.13(1.1), reasonable steps shall be taken to ensure that privileged communications between solicitors and clients are neither intercepted nor recorded.

24. That where there are grounds to suspect that if an authorization is granted, privileged communications between the targeted person and his solicitor will be intercepted, that fact shall be disclosed in the application to obtain an authorization.

25. That in a case to which Recommendation 21 applies, the authorization shall include a term that, so far as reasonably possible, privileged communications between the targeted person and his counsel not be intercepted or recorded.

Basket Clauses

26. That subject to Recommendation 27, the authorization shall contain a clause naming or otherwise identifying the persons the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence by reason of their involvement in the offence.

27. That, in addition, the authorization may contain a clause permitting the interception of a class of unidentified persons whose private communications there are reasonable grounds to believe may assist the investigation of the offence by reason of their involvement in the offence.

28. That subject to Recommendation 29, the authorization shall limit the interceptions to specified premises.

29. That the authorization may contain a clause permitting interception of private communications at other than specified premises where the other place is resorted to by persons known and identified in the authorization. At such premises, only those communications to which the known and identified person is a party may be intercepted, unless the specially designated agent has applied in writing to the authorizing judge as soon as practicable for amendment of the authorization. The application for an amendment shall be supported by the affidavit of a peace officer setting out the reasons for interception at these premises, the names of the persons whose communications are likely to be intercepted and the reasons why interception at such premises is required. The judge may refuse to amend the order, or amend the order, which amendment is effective from the date when interception commenced at the additional premises, unless the judge is not satisfied that the application was made as soon as practicable, in which case the amendment may be made effective at such later date as the judge sees fit in the circumstances.

30. That the legislation contain a list of terms or conditions which *may* be included in the authorization, such as the following:

(a) that periodic reports be made to the authorizing judge as to the identities of persons whose communications are being intercepted pursuant to a basket clause;

(b) that periodic reports be made to the authorizing judge as to the places, not specifically named in the authorization, where interceptions are taking place.

Surreptitious Entry

31. That the authorizing judge be given power to authorize an entry onto private premises without the consent of the occupier, for the installation, removal or servicing of an electromagnetic, acoustic, mechanical or other device.

32. That the authorizing judge may only so authorize where the circumstances of the offence are serious and there is a high degree of likelihood that relevant evidence will be obtained.

33. That an application for an authorization which includes an authorization to make a surreptitious entry shall state the reasons why such entry is required and why other less intrusive means will not be sufficient.

34. That it be an offence to enter private premises without the consent of the occupier for the purpose of installing, servicing or removing an electromagnetic, acoustic, mechanical or other device without an order under Part IV.1 of the *Criminal Code*, and an offence to remove anything from the premises at the time of the entry.

35. That the peace officer making the entry should not be entitled to use force against any person for the purpose of effecting such entry or exit, except as necessary to protect himself or others.

36. That the authorizing judge may order that certain means be used/not used to effect the entry.

37. That following the investigation, the owner and occupier of the premises be notified of the entry and be given a copy of the order which authorized the entry.

38. That reasonable steps be taken to repair any damage to the premises or to compensate the owner for any significant damage left unrepaired.

39. That the use of a small amount of electricity to enable the device to function shall not constitute a criminal offence.

Renewals

40. That where, to the knowledge of the designated agent or the deponent of the affidavit made in support of an authorization, an authorization has previously been granted in relation to the same or a related investigation, the application shall contain the information referred to in paragraph 178.13(3)(*b*) of the *Code*.

41. That a renewal of an authorization may include the names of persons previously provided for in the authorization but unnamed in the authorization.

42. That a renewal of an authorization may include additional places of interception of persons provided for in the original authorization.

43. That minor variations of the terms of the authorization may be included in a renewal, including the following:

(a) different or more accurate descriptions of persons or places;

(b) different or additional means of interception;

(c) different or additional offences clearly related to the offences in the original authorization and part of the same investigation.

44. That a renewal of an authorization may include terms not included in the original authorization, designed to minimize interceptions of communications which are not related to the offence.

45. That a renewal shall be for a period not exceeding thirty days, with the exception that where special cause is shown, a renewal may be for a period not exceeding sixty days. "Special cause" in this recommendation means circumstances making it probable that the investigation will not be completed within thirty days *and* it would be impracticable to obtain a further renewal within thirty days. Where the period of a renewal exceeds thirty days, the judge shall indicate on the face of the authorization the reasons therefor, with reference to the particular circumstances of the investigation.

46. That in any case referred to in Recommendation 45, the judge shall ensure that a renewal would not be available in the circumstances. In no case shall an authorization be granted where there is reason to suspect that it is intended to avoid the effect of Recommendation 45. Where the only reason that a renewal is unavailable is because the previous renewal or authorization has expired, then the subsequent authorization shall be for thirty days, unless special cause has been shown.

47. That the legislation provide for a list of terms and conditions which may be included in the renewal such as the following:

(a) that the interception shall terminate once the objective of the original authorization is achieved;

(b) that any applications for subsequent renewals or authorizations be made to the judge who granted the original authorization or renewal.

48. That section 178.14 of the *Criminal Code* be amended to include the following:

(a) in addition to the exceptions provided for in present paragraph (1)(*a*), to allow access to the material in the sealed packet for the purpose of dealing with an application for an authorization in related investigations;

(b) to permit the specially designated agent to retain a true copy of all the documents relating to an application made pursuant to section 178.12 or subsection 178.13(3).

49. That the prosecutor, when giving notice under subsection 178.16(4), shall include: a copy of the authorization and renewals under which the interceptions were made; and, subject to the order of a court, a copy of all the documents relating to an application for the authorization or renewal.

50. That prior to giving notice pursuant to subsection 178.16(4), the specially designated agent may apply to a judge as defined in section 482 of the *Criminal Code ex parte* and *in camera* for an order that certain portions of the material not be disclosed on the basis that disclosure could tend to reveal the identity of an informer or of any other person who has assisted with the investigation and in the latter case it is shown that it would not be contrary to the public interest that the identity of such persons be withheld. The application should be in writing and supported by the affidavit of a peace officer.

51. That the person against whom evidence is sought to be admitted pursuant to paragraph 178.16(1)(*a*) of the *Criminal Code* by reason of an interception made pursuant to an authorization or renewal, may apply at the preliminary inquiry or the trial to exclude that evidence and derivative evidence on the basis of a substantive defect in the application for the authorization or renewal. The following procedure would apply:

(a) The application should be in writing and supported by affidavit evidence (or *viva voce* evidence with leave of the judge).

(b) Only if the application and the evidence in support when considered together with the material disclosed under Recommendation 49 raises a real question as to whether there is a substantive defect in the application as defined in Recommendation 62 which could lead to the exclusion of evidence, shall the judge hold an inquiry as to the validity of the application for the authorization or renewal.

(c) Should the judge direct an inquiry, the burden of proof is on the Crown to satisfy the court that there was no substantive defect in the application as defined in Recommendation 62.

(d) The affidavit and testimony of the accused is not admissible at the instance of the Crown at the preliminary hearing or trial.

Emergency Authorization: Section 178.15

52. That section 178.15 be amended by the addition of subsection (6) as follows:

The admissibility of evidence acquired as a result of an order obtained under this section is not affected by the fact that the electromagnetic, acoustic, mechanical or other device was installed prior to the obtaining of the order, where the order under this section was obtained in relation to the offence under subsection 247(1) (kidnapping) and no private communications were acquired through use of the device until the order was obtained.

53. That an application for an emergency authorization under section 178.15 shall be made in writing or by telephone or other means of telecommunication and there shall be a record including: a statement of the reasons why an authorization could not, with reasonable diligence, be obtained under section 178.13; the facts relied upon to justify the belief that an authorization should be given, together with particulars of the offence; the persons whose private communications it is sought to intercept; and, the places of interception.

Admissibility of Evidence of Other Offences

54. That where the prosecution seeks to adduce primary evidence obtained by means of an authorization at the preliminary inquiry or trial of offences none of which are named in the authorization, the judge shall conduct a *voir dire* for the purpose of determining whether the interception of evidence of such offences was done in good faith.

55. That for the purposes of Recommendation 54, "good faith" means:

(a) that at the time of the authorization or renewal application, evidence of offences other than those specified in the application could not reasonably have been anticipated;

(b) that where evidence of other offences was anticipated, such offences were not named in the application because they were not offences for which an authorization could be obtained *and* they were not the primary focus of the investigation but *only incidental* to an investigation into offences named in the authorization;

(c) that at the time of the application or renewal, disclosure was made to the judge of the authorities to whom it was intended to give information obtained from the interception;

(d) that where the evidence is in relation to an offence for which an authorization could have been obtained and there were suspicions that evidence of

such offences would be obtained, those suspicions were disclosed in the material in support of the application *and* those offences were not named in the authorization only because

(i) the grounds for suspicions were not strong enough to meet the statutory test,

(ii) the investigation of such offences was not the primary focus of the investigation but *only incidental* to the primary investigation.

56. That where he is not satisfied that the interception of other offences was done in good faith, the judge shall exclude primary evidence and may exclude evidence shown to be derivative, where he is satisfied that to permit such evidence to be adduced would bring the administration of justice into disrepute.

Remedies: Admissibility of Evidence

57. That the reasonable notice referred to in subsection 178.16(4) apply whenever the prosecution seeks to introduce an intercepted private communication.

58. That where the prosecution has failed to give reasonable notice, a justice presiding at a preliminary inquiry or the trial judge may adjourn the proceedings for the purpose of requiring the prosecution to give reasonable notice and take whatever other steps are required to ensure that reasonable notice is given prior to the proceedings, taking into consideration the right of the accused to a trial within a reasonable time.

59. That section 457.3 be amended by including paragraph (*d*.1) as follows:

the justice may receive evidence of an intercepted private communication or evidence obtained as a result of an interception of a private communication apparently made under and within the meaning of Part IV.1, in writing, orally or in the form of a recording and, for the purposes of this section, section 178.16 does not apply to such evidence.

60. That primary evidence obtained by electronic surveillance be inadmissible unless:

(a) the interception was lawfully made

(i) with the consent of a party to the intercepted communication,

(ii) in accordance with the terms of an authorization;

(b) a party to the intercepted communication consents to the admission.

61. That where a defect exists on the face of the authorization or renewal, the trial judge shall admit the primary evidence obtained in apparent compliance with such authorization or renewal unless officers acting in apparent compliance therewith could not reasonably have believed that the authorization or renewal was valid.

62. That, for the purposes of Recommendation 51, a substantive defect in the application means that by reason of statements in the application or affidavit which to the knowledge of the investigators were false, or statements which were made recklessly without regard to their truth or falsity, or deliberate or reckless omissions, it is demonstrated that:

(a) none of the prerequisites set out in paragraph 178.13(1)(*b*) existed;

(b) reasonable and probable grounds to believe that a targeted offence was being committed by a person provided for in the authorization did not exist;

(c) any other grounds exist from which it may reasonably be concluded that, had the true state of affairs been known, the authorization would not have been granted, or not granted in substantially the form in which it was granted.

63. That evidence which is derived from primary evidence which is inadmissible, is itself inadmissible where in the opinion of the court, having regard to all the circumstances, to admit such evidence would bring the administration of justice into disrepute.

64. That evidence is derived from primary evidence where it would not have been obtained but for the acquisition of the primary evidence. However, evidence is not derivative where:

(a) it is obtained pursuant to an otherwise valid authorization although such authorization was based on evidence obtained as a result of an invalid authorization;

(b) it is the testimony of a witness to the commission of an offence although the witness' identity was discovered as a result of inadmissible primary evidence.

65. That once primary evidence is determined to be inadmissible, Crown counsel shall stipulate what, if any, evidence is derivative therefrom and the reasons why any other evidence is not derivative. That for the purposes of determining the validity of such reasons, the prosecution or the accused may, with leave of the court, call any witness for the purposes of cross-examination, and the accused with leave of the court may inspect any tapes or transcripts related to the investigation, whether or not he was a party to the communication.

66. That affidavit evidence be admissible and, in the absence of evidence to the contrary, be *prima facie* proof of:

(a) the times and places of the interception;

(b) the custody and continuity of the tape recordings;

(c) the manner of interception;

(d) service of notice.

67. That a copy of the authorization signed by a judge be admissible without proof of the authenticity of the signature.

68. That recital in the authorization as to the status of the designated agent be proof of such designation.

Notice under Section 178.23

69. That where notice under subsection 178.16(4) has not been given, a person who was the object of an interception shall be given notice of the dates of the interceptions and a copy of the authorization under which the interception took place.

70. That, upon written application by the accused, a judge with power to grant an authorization, or the trial judge, may require the prosecution to disclose such details of interceptions as may be necessary for an accused to make full answer and defence.

71. That, for the purposes of Recommendation 65, the judge may require the prosecutor to make such inquiries of law enforcement agencies as the judge considers necessary.

72. That notice under section 178.23 shall be given within ninety days of the termination of the authorization or renewal or such greater period not exceeding three years, where a judge is satisfied that by reason of a continuing investigation the giving of notice within ninety days would be contrary to the interests of justice.

73. That where notice cannot be given under section 178.23 because the person cannot be located, a peace officer with knowledge of efforts made to locate the person shall submit a statement in writing to the court setting out the reasons why notice has not been given and efforts made to locate the person.

The Disclosure of Intercepted Private Communications

74. That subsection 178.2(2) be amended expressly to exempt from the prohibition of subsection 178.2(1) the following:

(a) where the disclosure is made to a peace officer, the *Attorney General or his agent* and is intended to be in the interests of justice; and,

(b) where the disclosure is made to an investigative or law enforcement officer in a foreign jurisdiction and tends to reveal a past, ongoing or prospective crime in such jurisdiction.

75. That the authorizing judge be given express authority to order any person, including companies and organizations, engaged in providing communication or telecommunication services, as well as landlords, custodians or persons in charge of premises, to furnish all such technical or material assistance or information as may reasonably be required to accomplish the interception in accordance with the authorization, and to be compensated therefor at the prevailing rates.

76. That failure of compliance in accordance with the authorization shall be punishable as contempt of court.