Dalhousie Law Journal

Volume 10 | Issue 3 Article 15

1-1-1987

Electronic Surveillance in Crime Detection: An Analysis of Canadian Wiretapping Law

Norman MacDonald
Dalhousie University

Norman MacDonald*

Electronic Surveillance in Crime Detection: An Analysis of Canadian Wiretapping Law

I. *Introduction*

Wiretapping and electronic surveillance by law enforcement agencies has been going on in Canada for decades. An inquiry by the McDonald Commission in 1981 reveals this as part of normal activities of the Royal Canadian Mounted Police.[1] Now new technologies have enlarged the capacity of police in the surveillance area. Some of these developments include:

1) Laser beams and electronic rays capable of picking up and transmitting voices in the room when aimed at a wall or window.
2) Miniature listening devices known as "bugs". Once installed these devices can overhear and record everything in the room and transmit up to half a mile away.
3) Miniature microphones that can be worn on an individual who engages in conversation with the suspect.
4) Wiretapping — the interception of telephone communications. This involves a connection to the wires over which conversation is taking place.
5) Parabolic microphones that can overhear without being placed in the premises.
6) Combination mirror — transmitter capable of picking up both sight and sound.[2]

The thought of police abuse and government interference with individual privacy is not far fetched. The possibility of being a target of electronic surveillance is frightening. Hence a discussion of the relevant law in this area is desired.

1. *Summary*

At present some of the most technologically advanced equipment capable

---

*LL.B. Dalhousie, 1986. The original version of this article was prepared in the context of a seminar on law and technology taught by Professor Bankier at Dalhousie University.

1. Canada, *Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police — Second Report* (2 vols. 1981), vol. 1, (hereafter McDonald Commission Second Report).

2. See *Berger* v. *New York* 388 U.S. 41 (1967); Manning, *The Protection of Privacy Act, Bill C-176* (Toronto: Butterworths, 1974): Watt, *Law of Electronic Surveillance in Canada* (Toronto: Carswell, 1979).

of keeping an individual under auditory and visual surveillance indefinitely is available to law enforcement agencies in Canada. The *Protection of Privacy Act*[3] which forms Part IV.I of the *Criminal Code*[4] under the title of "Invasion of Privacy" sets out authorization criteria for police officers and law enforcement personnel in using such devices. In addition electronic surveillance can be carried on completely outside the ambit of judicial control, as described in Part IV.I, by obtaining a warrant under the *Official Secrets Act*[5].

It is clear then that in enacting the *Protection of Privacy Act* Parliament recognized for the first time an individual's right to privacy while at the same time allowing state sanctioned electronic eavesdropping for the purpose of crime detection. The study of electronic surveillance must therefore involve an analysis of competing interests between the individual and the state. On the one hand the individual has a right to privacy. Use of electronic surveillance devices by government agencies could lead us into a "1984" type of society where "Big Brother" is watching everything.[6] On the other hand the state has an interest in protecting its citizens from criminals and criminal activities.

The purpose of this essay is to examine the law of electronic surveillance in crime detection and how this relates to the privacy of the individual. In doing so it is necessary to take a look at the history of eavesdropping laws in Canada as well as the provisions of the *Protection of Privacy Act.*[7] An analysis of relevant case law in this area should be useful in determining if the Act is operating in accord with the policies behind it. Finally, the future of electronic surveillance in Canada will be discussed.

II. *History of Eavesdropping Laws in Canada*

Prior to the *Protection of Privacy Act*[8] there was no legislation to regulate and control the use of electronic surveillance devices by law enforcement personnel. At common law eavesdropping was recognized as a nuisance offence.[9] One could therefore argue that this could be applied against law enforcement people who engage in electronic surveillance. The practice of eavesdropping, however, does not seem to have ever been regarded as an indictable offence. In *R.* v. *Mason*,[10] one of the first Canadian cases on

3. S.C. 1973-74, c. 50.
4. R.S.C. 1970, c. C-34, as amended.
5. R.S.C. 1970, c. 0-3, as amended.
6. see George Orwell's *1984.*
7. S.C. 1973-74, c. 50.
8. S.C. 1973-74, c. 50.
9. 4 Blackstone Commentaries, 168 (Lewis ed., 1897).
10. (1918), 39 D.L.R. 54 (Que. P.M.C.).

eavesdropping, it was held that eavesdropping was not a common law offence in Canada and was therefore not punishable. Further, in *The King* v. *County of London Quarter Sessions Appeals Committee, Ex. p. Metropolitan Police Commission*, Lord Goddard stated that "no instance can be found in the books of any indictment being preferred for this offence at common law".[11] This case was later applied in *Re Copeland and Adamson*[12] where an application to prohibit police wiretapping was denied on the grounds that it was neither an offence nor was there any common law right to privacy. Grant J. was of the view that it was for Parliament to impose limitations on wiretapping and not the courts.

The only federal legislation dealing with intercepting private communicatons at that time was s. 25 of An Act to Incorporate the Bell Telephone Company of Canada[13] which read:

> Any person who shall willfully or maliciously injure, molest or destroy any of the lines, posts or property of the Company, or in any way willfully obstruct or interfere with the working of the said telephone lines, and intercept any message transmitted thereon shall be guilty of a misdemeanor.

This statute, however, was never used to prohibit police officers from engaging in wiretapping nor to prosecute anyone who tapped a telephone. In *Re Copeland and Adamson*[14] Grant J. held that although s. 25 makes it an offence to "interfere with" or to "intercept" telephone conversations, wiretapping could not be an offence within the meaning of that section since it does not impede or disturb a telephone conversation and in any event police officers acting with reasonable and probable grounds are justified in doing whatever they are required to do under the *Criminal Code*. He then went on to review the *Privacy Act*[15] of British Columbia which created a tort, actionable without proof of damage, against anyone willfully and without claim of right to violate the privacy of another. The legislation specifically provided that privacy may be violated by eavesdropping or surveillance whether or not accompanied by trespass.[16] There were, however, exemptions from liability for peace officers acting in the course of their duty.[17] In refusing to be influenced by the British Columbia legislation Grant J. held that no other province in Canada allows a right of privacy *per se* or a remedy for the breach thereof.

---

11. (1948) 1 K.B. 670 at 675 (C.A.).
12. (1972), 28 D.L.R. (3d) 26 (Ont. H.C.).
13. S.C., 1880 43 Vict. c-67.
14. *Supra,* note 412.
15. S.B.C. 1968, c. 39.
16. *Id.* s. 2(3).
17. *Id.* s. 3(1).

Other provinces began to establish privacy and telephone legislation in the late 1960's and early 70's. Provincial privacy legislation, like that of British Columbia, created a tort, actionable without proof of damage, for anyone willfully and without claim of right, to violate the privacy of another.[18] Telephone legislation created an offence, punishable on summary conviction, for anyone unlawfully interfering with telephone company equipment.[19] While electronic surveillance was covered in both types of legislation, police officers acting in execution of their duty, as in British Columbia, were exempt from liability. In fact, telephone companies cooperated with law enforcement agencies in tapping telephone lines.

Usually the only bodies regulating police wiretapping activities were the provincial Police Commissions who set guidelines for electronic surveillance. This required that the officer had reasonable and probable grounds for conducting a wiretap and that the Chief of Police gave his permission.[20] The officer requesting a wiretap would go to his immediate supervisor who then went to the Chief of Police to get it authorized. Hence, we had a situation where the police were policing themselves. Sometimes officers would act on their own initiative without informing or getting approval of those in command. This was discovered by the McDonald Commission's investigation into R.C.M.P. activities.[21] The Royal Canadian Mounted Police officially maintained a policy against wiretapping yet nevertheless it went on. It appears that any controls maintained were very slack.

Disturbed about possible police abuses that may have been going on, Parliament, in the late 1960's and early 70's, set up committees to study the matter of electronic surveillance. The first of these committees was the Canadian Committee on Corrections (hereafter called the Ouimet Committee). The Ouimet Committee realized that wiretapping was commonly used by police forces in criminal investigations and that there was no control over their activities. The Committee was of the view that federal legislation controlling the use of wiretapping by police forces should be implemented. In addition they recommended that wiretapping and electronic eavesdropping for criminal purposes should be outlawed but that there should be an exception for law enforcement purposes subject to strict controls.[22]

---

18. *The Privacy Act,* S.M. 1970, c. 74; S.S. 1973-74, c. 80.
19. *The Telephone Act,* S.M. 1970, c. 74; R.S.O. 1970, c. 457; *The Alberta Government Telephone Act,* R.S.A. 1970, c. 12; *The Rural Telephone Act,* R.S.N.S. 1967, c. 273.
20. Interview, Cpl. F. Baisley, Halifax Police Dept., (Nov. 1984); *Re Copeland and Adamson, supra,* note 11.
21. McDonald Commission Third Report, (1981).
22. Canada, *Report of the Canadian Committee on Corrections* (1969), at 83.

The House of Commons Standing Committee on Justice and Legal Affairs studied the matter in 1970 and made several recommendations that were adopted including:

1) Wiretapping and electronic eavesdropping should be made criminal offences.
2) Only specified crimes should be subject to electronic surveillance.
3) There should be stringent controls and defined limits on police use of electronic surveillance.
4) Procedures for applications to use electronic devices and obtaining judicial authorization.
5) There should be a time limit on how long the devices can be used.
6) A yearly report to Parliament by the Attorney General.[23]

In addition the Task Force on Privacy and Computers studied the area of privacy in relation to wiretapping and concluded that the privacy of the individual should be balanced against social and political values.

The result of these studies led to the introduction of the Bill on Privacy.[24] After dying on the order paper twice and after adopting many recommendations from the Standing Committee on Justice and Legal Affairs, The *Protection of Privacy Act*[25] was finally passed and came into effect on June 30, 1974. The Act was modelled after Title III of the *Omnibus Crime Control and Safe Streets Act of 1968*[26] (hereafter referred to as Title III), its American counterpart legislation. The Act remained in its original state for three years until significant changes were made with the passage of ss. 7 to 12 of the *Criminal Law Amendment Act, 1977*[27].

III. *The Protection of Privacy Act*[28]

1. *General Outline of the Act*

The *Protection of Privacy Act* was Parliament's attempt to recognize an individual's right to privacy by making it illegal to intercept a person's conversations without that person's consent. At the same time, however, Parliament recognized the utility of electronic surveillance in crime detection and created exemptions from liability for law enforcement

---

23. Canada, Standing Committee on Justice and Legal Affairs, *Fourth Report* contained 8 in the minutes and proceedings of the Standing Committee on Justice and Legal Affairs, No. 7, February 5, 1970, 2nd Session, 28th Parliament No. 7:7.
24. Manning, *supra,* note 2 at 1-2.
25. S.C. 1973-74, c. 50.
26. 18 U.S.C. ss. 2510-20 (1970), originally enacted as Act of June 19, 1968, Pub. L. No. 90-351, ss. 802, 82 Stat. 212.
27. S.C. 1976-77, c. 53.
28. S.C. 1973-74, c. 50, as amended.

purposes. The resulting new Act amended the *Criminal Code*,[29] the *Crown Liability Act*[30] and the *Official Secrets Act*[31]. These amendments will now be examined.

(a). *Amendments to the Criminal Code*

The Protection of Privacy Act added a new part, Part IV.I, entitled "Invasion of Privacy" to the *Criminal Code*.[32] This part created three new indictable offences those of i) willfully intercepting a private communication by means of electronic devices ii) possessing, selling or purchasing these devices knowing that they are designed for interception of private communications and iii) disclosing information that has been intercepted by means of these devices without the consent of the object of the interception (ss. 178.11, 178.18 and 178.20 respectively). The maximum penalties provided are, five years imprisonment, in the case of a wilful interception, and two years for the other offences. The additional penalty sections allow for the forfeiture of any devices used as well as an award for punitive damages up to a maximum of $5000. (ss. 178.19, 178.21). However, the offence creating sections provide exemptions from any liability for law enforcement personnel.

In order to be exempt from liability, a police officer must either have the consent of the party whose communication was intercepted or be authorized to conduct an interception. The Act sets out steps to be followed to obtain judicial authorization both to initiate and continue electronic surveillance (ss. 178.12 to 178.15 inclusive). The judge must be satisfied that to grant an authorization order would be in the best interests of the administration of justice or that other investigative techniques have been tried and failed and are unlikely to succeed or that it would be impractical to use other investigative procedures. The authorization order must contain details of the interception and is only valid for a period not exceeding sixty days. The authorization can of course be renewed but again each renewal period cannot exceed sixty days. All of the documents related to the application of authorization are placed in a sealed packet and kept in a secret place until ordered opened by a judge. The regular procedure can be by-passed in the case of an emergency but in such a case the authorization is only valid for up to 36 hours.

The Act also provides evidentiary rules in respect of both evidence of intercepted private communications and evidence obtained either directly

29. R.S.C. 1970, c. C-34, as amended.
30. R.S.C. 1970, c. C-38, as amended.
31. R.S.C. 1970, c. 0-3, as amended.
32. R.S.C. 1970, c. C-34, as amended.

or indirectly as a result of information acquired through the interception (ss. 178.15, 178.16 and 178.17). Evidence is only admissible where the interception was lawfully made or where there is consent to its admission. Notwithstanding this provision, the judge has a discretionary power to admit evidence that would otherwise be inadmissible if it is relevant and if the only reason for not allowing it is because of a defect in form or procedure in applying for the authorization.

In addition, the Act contains reporting sections requiring the Solicitor General of Canada and the provincial Attorney General to publish annual reports disclosing the extent of court authorized interceptions (s. 178.22) as well as requiring that notice be given to the objects of interception within 90 days after the expiry of the authorization (s. 178.23). Section 178.23 provides that the judge can grant a delay before notification must be given and also provides for exemption from the notification requirement where the interception is made pursuant to a warrant under the *Official Secrets Act*[33].

The provisions of Part IV.I as well as the difficulties that have been encountered in its operation will be discussed in more detail later in the text.

(b). *Amendments to the Crown Liability Act*

The *Protection of Privacy Act* adds a new part, Part I.1 to the *Crown Liability Act*[34]. This allows for civil liability to be imposed upon the Crown where a Crown servant, by means of electronic surveillance, intentionally intercepts a private communication or discloses information that has been intercepted, in the course of his employment (ss. 7.2 and 7.3 respectively). The Crown is liable for all loss or damage caused by or attributable to such an interception and, if no award has been made to the plaintiff under section 178.21 of the *Criminal Code*[35], for punitive damages not exceeding five thousand dollars.

Just as there are saving provisions in the *Criminal Code*[36] the *Crown Liability Act*[37] also provides exemptions from liability. In the case of an intentional interception (s. 7.2) the Crown is not liable where the interception was either i) lawfully made ii) was made with the consent of the originator or the person intended to receive the private communication or iii) or was made by a Crown servant in the process of random radio monitoring.[38] The term "lawfully made" has been held to mean an

33. R.S.C. 1970, c. 0-3, as amended.
34. R.S.C. 1970, c. C-38, as amended.
35. R.S.C. 1970, c. C-34, as amended.
36. R.S.C. 1970, c. C-34, as amended.
37. R.S.C. 1970, c. C-38, as amended.
38. *Crown Liability Act,* R.S.C. 1970, c. C-38, s. 7.2(2).

interception that has been made in accordance with any of the exemptions provided in s. 178.11(2) of the Code.[39] Thus a person acting in good faith who aids in any way a person whom he has reasonable and probable grounds to believe is acting with an authorization is exempt from liability.[40]

In the case of an intentional disclosure of information obtained by use of electronic surveillance, the Crown can avoid liability if the disclosure took place under the following circumstances:

i) with the express consent of the originator or the person intended to receive the private communication;
ii) in the course of giving evidence in any civil or criminal proceedings;
iii) in the course of any criminal investigation if the private communication was lawfully intercepted;
iv) in giving notice under s. 178.16 of the Code or furnishing further particulars pursuant to an order under s. 178.17;
v) in the course of random radio monitoring;
vi) where disclosure is made to a peace officer in the interest of the administration of justice.[41]

There is very little authority interpreting the provisions of Part IV.I with respect to civil liability but it is clear that civil liability was not intended to apply to law enforcement personnel that conduct electronic surveillance with the requisite authorization.

(c). *Amendment to the Official Secrets Act*

The amendment to the *Official Secrets Act*[42] adds a new section, section 16, which allows the Solicitor General of Canada to issue a warrant authorizing the interception or seizure of "any communication" where he is satisfied that it is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or that it is necessary for the purpose of gathering foreign intelligence essential to the security of Canada.[43] The provisions of this amendment fall outside the ambit of both Part IV.I and the *Crown Liability Act*.[44] The warrant may be issued to any individual and is not limited to police officers. It is probable that such a warrant will be issued to agents of the new civilian Security Service formed under the *Canadian Intelligence*

---

39. *R* v. *Cremascoli* (1977), 38 C.C.C. (2d) 212 at 218 (Ont. C.A.).
40. *Criminal Code*, R.S.C. 1970, c. C-34, s. 178.11(2)(b).
41. *Crown Liability Act*, R.S.C. 1970, c. C-38, s. 7.3(2).
42. R.S.C. 1970, c. 0-3, as amended.
43. R.S.C. 1970, c. 0-3, as amended, s. 16(2).
44. R.S.C. 1970, c. C-38, as amended.

Security Service Act.[45] There is no limit to the length of time that such a warrant will be in force.

The amendment gives a wide meaning to the term "subversive activity". Under s. 16(3) subversive activity includes:

(a) espionage or sabotage;
(b) foreign intelligence activities directed toward gathering intelligence information relating to Canada;
(c) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means;
(d) activities by a foreign power directed toward actual or potential attack or other hostile acts against Canada; or
(e) activities of a foreign terrorist group directed toward the commission of terrorist acts in or against Canada.[46]

The Amendment provides that a warrant issued under this Act shall contain details of the interception including the type of communication to be intercepted, the persons who may make the interception and the length of time the warrant is to be in force.[47]

There is also a reporting section requiring the Solicitor General to prepare an annual report to Parliament detailing the number of warrants issued, the average length of time that a warrant was in force, the methods of interception used, and an assessment of the importance of the warrants issued.[48] The difference between this section and the reporting sections of Part IV.I is that the annual report under this Act contains less information and there is no notice requirement to the objects of interception.

This amendment seems to be more in favour of electronic surveillance with minimal controls than Part IV.I. The Act allows the by-passing of regular procedures for obtaining judicial authorization to conduct electronic surveillance. There is no control as to the form and substance the applications for authorization must take. For example there is no provision that there must be a formal written application with an accompanying affidavit from the applicant as in Part IV.I. The application and subsequent granting of the authorization is not limited to designated agents as in Part IV.I. Anyone can apply for and obtain a warrant. There is no limit on the length of time that a warrant can be in force. All of these factors are at the discretion of the Solicitor General.

---

45. S.C. 1984, c. 21.
46. *Official Secrets Act*, R.S.C. 1970, c. 0-3, as amended, s. 16(3).
47. *Official Secrets Act*, R.S.C. 1970, c. 0-3, as amended, s. 16(4).
48. *Official Secrets Act*, R.S.C. 1970, c. 0-3, as amended, s. 16(5).

As to the circumstances under which a warrant can be issued, the definition of "subversive activity" covers such a wide area that it could conceivably apply to almost anything. For example "activities directed toward accomplishing a governmental change"[49] could include many of the peaceful demonstrations that go on in Canada today such as anti-nuclear or anti-abortion protests. Similarly the other provisions defining subversive activity are quite vague and could be interpreted as the Solicitor General of the day sees fit.

The evidentiary rules provided in Part IV.I are not applicable under the *Official Secrets Act*.[50] This means that an interception does not necessarily have to be one which is lawfully made in order to be admissible as evidence. Further, there is no provision requiring that particulars of the interception as well as notice that it will be presented at trial must be given to the accused. Under Part IV.I failure to comply with these terms will result in the evidence being inadmissible.[51].

Section 16 of the *Official Secrets Act*[52] is probably the most frightening of the three amendments since it contains virtually no controls regarding the interception of private communications. In fact it can be used to intercept any communication. While Part IV.I also condones electronic surveillance it does so while maintaining safeguards for individual privacy.

2. *Part IV.I — Invasion of Privacy*

Part IV.I of the *Criminal Code*[53] allows for the interception of private communications by means of electronic surveillance where it is done for law enforcement purposes and under judicial authorization. However, electronic surveillance can still be carried on without judicial authorization if it is done with the consent of one of the parties of interception or if the surveillance activity falls outside the scope of the Act.

(a). *Electronic Surveillance Without Judicial Authorization*

Before the judicial authorization criteria of Part IV.I must be followed, the surveillance activity must fall within the scope of the Act. If the activity does not come within the definitions in Part IV.I then authorization is not required. This section will take a look at the relevant definitions as well as the consent provision of Part IV.I.

---

49. *Official Secrets Act*, R.S.C. 1970, c. 0-3, as amended, s. 16(3)(c).
50. R.S.C. 1970, c. 0-3, as amended.
51. Part IV.I, s. 178.16(4).
52. R.S.C. 1970, c. 0-3, as amended.
53. R.S.C. 1970, c. C-34, as amended.

(i) *Private Communication Requirement*

Before a police officer is required to get judicial authorization to conduct electronic surveillance, the communication in question must be such that it falls within the definition of a private communication which is:

> 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.[54]

The test then appears to be an objective one requiring a *reasonable* expectation of privacy from the originator. However, courts have also utilized a subjective element looking to the mind of the originator. In *R.* v. *Carothers; Richardson* v. *Brunhoffer*[55] the originators suspected that their telephone was tapped but continued to use that method of communication. The trial judge held that as soon as the suspicion became manifest the communication was no longer "private" as defined in Part IV.I. However, just because the originator has a suspicion, this does not necessarily mean that the communication is no longer a private one. If the originator can reasonable expect that his communication will not be overheard then it is a private communication. In determining the reasonable expectation one must consider the surrounding circumstances. Mr. David Watt, Senior Crown Counsel with the Ontario Attorney-General's Department, has summarized the law in this area in his treatise:

> Whether any given communication asserted to fall within the definition of "private communication" in Part IV.I does so, will depend upon the circumstances surrounding its making. It would seem obvious that statements uttered for public consumption in a public forum, or to public officials would provide the clearest example of a statement beyond the reach of Part IV.I. Equally, in relation to the subjective expectation of privacy, a communicant who chooses a method of communication which exposes his statements to uninvited ears can scarcely assert a reasonable expectation of privacy in response to his implicit invitation to listen. Absent circumstances negating the subjective expectation of privacy of the originator of the statements, the inquiry then shifts to the reasonable expectation of privacy, a matter of inference in light of all relevant facts and circumstances. Relevant considerations include the location, content and purpose of the communication, the means by which it is transmitted, and the nature of the means, or techniques, if any, employed by the originator to prevent being overheard.[56]

Central to the issue of private communication is who can be regarded as an originator. In *R.* v. *Miller and Thomas (No. 1)*,[57] the court held that

54. Part IV.I, s. 178.1.
55. [1978] 6 W.W.R. 571 (B.C. Co. Ct.).
56. Watt, *Law of Electronic Surveillance in Canada* (Toronto: Carswell, 1979).
57. (1975), 28 C.C.C. (2d) 94 (B.C. Co. Ct.).

the person making the telephone call in question is the originator. In face to face conversations it has been held that the person who speaks first is the originator. However, the Supreme Court of Canada has recently defined the originator as "the person who makes the remark or series of remarks which the Crown seeks to adduce as evidence".[58] Thus if an undercover police officer speaks first in a face to face conversation he cannot be regarded as the originator, and therefore his consent to the interception is irrelevant.

(ii). *Interception Requirement*

Another condition which must exist before the provisions of Part IV.I can be invoked is that the communication must have been intercepted. Under Part IV.I this means:

> listen to, record or acquire a communication or acquire the substance, meaning or purport thereof.[59]

There have been several interpretations of what constitutes an interception. In *R.* v. *McQueen*[60] a police officer answered several telephone calls and took certain bets during a raid on a room alleged to be a common betting house. Under a strict interpretation of the Act the trial judge invoked the exclusionary provisions of s. 178.16(1) on the grounds that the lack of both consent on the part of the originator or the person intended to receive the communication and the lack of judicial authorization resulted in an illegal interception and the evidence was therefore inadmissible. On appeal it was held that the trial judge erred in excluding the evidence since there had not been an interception of a private communication. McDermid J.A. concluded that in absence of any interference between the place of origination and the intended destination of the communication there could not be an interception. The exclusionary provisions of Part IV.I could not be invoked as long as the originator intended the person who answered the telephone to receive the message. The fact that he was mistaken as to the identity of the receiver is irrelevant.[61]

Other authorities suggest that the element of a third party is essential to an interception. In *R.* v. *Dunn*[62] a police officer listening on an extension telephone, with the consent of the intended recipient, heard the originator utter death threats and obscenities. The court found that the fact that the caller did not identify the recipient other than by her voice,

58. R v. *Goldman* (1980), 13 C.R. (3d) 228 at 248 per McIntyre J. (S.C.C.).
59. Part IV.I, s. 178.1.
60. (1975), 25 C.C.C. (2d) 262 (Alta. C.A.).
61. *Supra,* note 59 at 265-66.
62. (1975), 33 C.R.N.S. 299 (N.S. Co. Ct.).

suggested that he did not expect another person to be listening in. Accordingly he found that there had been an interception within the terms of Part IV.I.

In the United States difficulties in interpreting the word "intercept" do not occur as readily as under Part IV.I since Title III offers a broader definition. Title III defines intercept as:

> The aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical or other device.[63]

Under this definition an interception has been held to involve the overhearing of a communication in which the eavesdropper is neither a participant nor an intended listener.[64] Using this interpretation, an accused would only need to show a reasonable expectation of privacy before invoking the prohibitory and exclusionary provisions of Part IV.I, provided of course the interception itself was illegal.

(iii). *The Requirement of an Electromagnetic, Acoustic, Mechanical or Other Device*

Another necessary element before Part IV.I can come into play is that the interception must have occurred by use of an "electromagnetic, acoustic, mechanical or other device". This is defined as:

> 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.[65]

While it appears that this definition could include everything other than a hearing aid, there have been difficulties in interpretation. In *R.* v. *McQueen*[66] it was held that there had been no electromagnetic, acoustic mechanical or other device involved when a police officer answered incoming calls at a gaming house. In *R.* v. *Dunn*[67], however, listening in on an extension telephone was held to involve such devices. The two decisions are difficult to reconcile since it appears that an ordinary telephone does not fall within the above definition yet an extension telephone does.

Another definition problem is raised in cases involving interception by use of video devices. In *R.* v. *Irwin and Sansome et al.*[68] evidence of illegal gambling was obtained through the use of a closed circuit video camera and a wireless microphone. The trial judge rejected the evidence

63. Title III, s. 2510(4).
64. *U.S.* v. *King* 335 F. Supp. 523 (S.D. Cal., 1971).
65. Part IV.I, s. 178.1.
66. *Supra,* note 60.
67. *Supra,* note 62.
68. (1975), 32 C.R.N.S. 398 (ont. C.A.).

under Part IV.I. On appeal this was held to have been improperly rejected since the evidence had been obtained prior to the passage of Part IV.I.

Since then there does not appear to be any cases deciding whether video surveillance involves the use of an electromagnetic, acoustic, mechanical or other device. Watt submits that video surveillance without any sound recording does not fall within the ambit of Part IV.I.[69] However, the definition of private communication under Part IV.I includes any telecommunication. Under the *Interpretation Act*[70] telecommunication means:

> any transmission, emission or reception of signs, writing or images or intelligence of any nature by wire, radio, visual or other electromagnetic system.

This definition of telecommunication could be used to include video surveillance.

(iv). *Electronic Surveillance with the Consent of a Party*

An interception without judicial authorization can still be carried out where the originator of the private communication or the person intended to receive it has given his consent, express or implied, to the interception.[71] The consent must be free and voluntary and not extracted through coercion.[72] However, consent given for fear of going to prison is valid. In *R.* v. *Rosen*[73] consent had been given by co-conspirators as part of a plea bargain to avoid imprisonment. The court held that the impurity of the motives for consenting did not vitiate the consent as long as it was given free of duress and coercion. Thus if a conspirator consents due to favours offered him by the Crown, then the consent is still valid.

Even where consent to intercept the communication has been given there are still evidentiary difficulties involved. Under s. 178.16 an intercepted communication is inadmissible as evidence unless lawfully made or the originator or person intended to receive the communication has expressly consented to the admission. In *Goldman,* the question of whether a further consent to admission was needed arose. The court held that the consent obtained under s. 178.11 made the interception one which was "lawfully made" and therefore no further consent was required to admit the intercepted communication as evidence.

---

69. Watt, *supra,* note 56 at 48.
70. R.S.C. 1970, c. I-23, s. 28.
71. Part IV.I, ss. 178.11(2)(a), 178.11(3).
72. *R. v. Goldman, supra,* note 58 at 250.
73. (1976), 30 C.C.C. (2d) 565 (Ont. H.C.).

Having the consent of one of the parties turns what otherwise would be an illegal activity into a legal one. Hence, there is no need to obtain judicial authorization. Similarly, if the surveillance activity does not fall within the definitions in s. 178.1 then the provisions of Part IV.I do not apply. In all other cases judicial authorization is required.

(b). *Electronic Surveillance With Judicial Authorization*

An interception of a private communication can be lawfully made if it is authorized by a judge of a superior court having criminal jurisdiction or a judge as defined in s. 482 of the *Criminal Code*.[74] The procedural provisions setting out steps to be followed to obtain authorization both to initiate and continue electronic surveillance are found in ss. 178.12 to 178.15 inclusive.

There are two types of authorizations that can be given. These are:

1) The conventional authorization obtainable on an *ex parte* application for a period not exceeding sixty days;[75]
2) An emergency authorization obtainable on an *ex parte* application to a designated judge for a period of up to 36 hours.[76]

In addition the conventional authorizations can be renewed for periods of sixty days at a time under s. 178.13(4).

The procedure that is followed is basically the same throughout Canada. The peace officer, who has been specially designated, presents a written application along with an affidavit to the judge. If everything is in order the judge will usually grant an authorization order premitting the communications of the named and unnamed individuals to be intercepted for a specified period of time. A similar procedure follows the renewal process. All material related to the application, except the authorization or renewal order, is sealed in a packet and kept in a secret place in the custody of the court.

There are formal requirements that must be followed in order to get an authorization. First, the application must come from the provincial Attorney General or the Solicitor General of Canada or one of their agents specially designated in writing. For criminal offences the application must come from the Attorney General or one of his agents. For conspiracies to violate federal statutes as well as any remaining offences, the applications must come from the Solicitor General's people.[77]

---

74. R.S.C. 1970, c. C-34, as amended.
75. Part IV.I, s. 178.13(2).
76. Part IV.I, s. 178.15(2).
77. Part IV.I, s. 178.12(1).

Accompanying the application must be the affidavit of the agent stating among other things:

1) the offence in respect of which the interception is sought;
2) the identity, if known, of the person(s) whose communication is to be intercepted;
3) a description of the premises at which the interception will be intercepted as well as the location;
4) a description of the manner of interception to be used; and
5) whether other investigative techniques have been tried and failed or why it appears unlikely that they will succeed.[78]

In addition the affidavit and the authorization order must contain reference to individuals whose identities are not known if the police wish to lawfully intercept communications of those who may use the same premises as the named person.

In granting the authorization the judge is not obliged to state his reasons for doing so although he must be satisfied that it would be in the best interests of the administration of justice or that other investigative procedures have been tried and have failed or that they are unlikely to succeed.[79] Having met all of these requirements the judge will grant the authorization order although he can request more information before doing so.

A renewal application follows the same procedure and is viewed as an extension of the original application. It cannot include new objects of interception or new offences or else it is treated as an original application.

Once an authorization has been granted all documents related to the application, except for the authorization or renewal order, are placed in a packet and sealed by the judge to whom the application was made. The documents are then kept in the custody of the court in a place to which the public has no access and cannot be opened except for dealing with a renewal or pursuant to an order from a superior court judge of criminal jurisdiction.[80]

Pursuant to s. 178.23 notice of an interception must be given to the parties in question within 90 days after the expiry of the authorization or its renewal. This does not apply in the case of a warrant under the *Official Secrets Act*,[81] however.

Thus the *Protection of Privacy Act*[82] has resulted in state sanctioned electronic surveillance for the purpose of crime detection. The

---

78. *Id.*
79. Part IV.I, s. 178.13.
80. Part IV.I, s. 178.14.
81. R.S.C. 1970, c. 0-3.
82. S.C. 1973-74, c. 50.

amendments to the *Criminal Code*[83] and the *Official Secrets Act*[84] raise some serious questions that should be addressed in light of basic policy considerations.

IV. *Policy Considerations*

When the House of Commons and the Standing Committee on Justice and Legal Affairs studied the matter of electronic surveillance in crime detection, they recognized that the provisions of the proposed Act touched on delicate areas. The Act was a political bombshell at the time and was passed on the basis that if there were difficulties in its operation certain provisions could be changed. The Act has been in effect now for over ten years and many difficulties have been encountered in the way the provisions have been carried out. Accordingly, it is necessary to examine the policies behind the Act to see if they are being carried out.

1. *Purpose and Intent of the Act*

The general purpose of the Act was to increase the protection of privacy in Canada by making it illegal to intercept private conversations unless done so in an authorized manner for law enforcement purposes. Parliament recognized the utility of electronic surveillance in crime detection and so it created exemptions from liability for the purpose of law enforcement. The Act set out procedures that had to be followed before an interception could be lawfully made. Thus Parliament tried to create a balance between individual privacy and the state's maintenance of law and order.

The question then arises as to whether the Act functions in accordance with the purposes for which it was designed. Is the balance between the individual and the state being effectively maintained? We have already seen situations where electronic surveillance can be lawfully carried out without any authorization. This seems to conflict with Parliament's intent of maintaining strict controls over the use of such surveillance devices by law enforcement personnel. In addition there are operative provisions of the Act that conflict with the intent of Parliament. These defects occur under both the *Criminal Code*[85] and the *Official Secrets Act*.[86] They will now be examined.

2. *Conflicts With the Intent of Parliament*

Certain provisions of the Act and the way they are being carried out

83. R.S.C. 1970, c. C-34, as amended.
84. R.S.C. 1970, c. 0-3, as amended.
85. R.S.C. 1970, c. C-34, as amended.
86. R.S.C. 1970, c. 0-3, as amended.

infringe too greatly on the privacy of the individual. This is in direct conflict with Parliament's intent to maintain a balance between individual privacy and law enforcement. The scales have been tipped in favour of our police forces. Accordingly, it is necessary to discuss these provisions.

(a). *Offences in Which Electronic Surveillance Can Be Used*

When the Standing Committee on Justice and Legal Affairs was studying the matter, they sought to limit the use of electronic surveillance to "serious crimes that threaten life and individual and group well being to such an extent that the protection of privacy must yield to protection against anti-social activities"[87]. The provisions of the present Act, however, list over fifty offences in Part IV.I[88] as well as giving a wide discretion to conduct surveillance under the *Official Secrets Act*[89] where there is a threat to national security. This clearly goes beyond the proposals of the Standing Committee.

Since the American parallel, Title III, was the model for the present Act, it is useful to look at the comparative legislation. Under Title III there is also a lengthy list of crimes in respect of which electronic surveillance can be used. This probably explains the similar feature in our Canadian legislation. Policy makers in the United States, however, have been debating the issue of electronic surveillance longer than their Canadian counterparts. In limiting the scope of such law enforcement tools, the American Bar Association also felt that electronic surveillance should be limited to serious crimes.

In helping define what constitutes a "serious" crime for which electronic surveillance should be used, the British Royal Commission on Criminal Procedure sets the following guidelines:

> Whether a particular coercive power should be available in respect of a particular offence will vary to some extent with the nature of the offence and the way in which it is likely to be investigated. In our view the following categories of offence (including where appropriate, attempts or conspiracies to commit those offences) should be covered: serious offences against the person or serious sexual offences (murder, manslaughter, causing grievous bodily harm, armed robbery, kidnapping, rape); serious offences of damaging property (arson, causing explosions); serious dishonesty offences (counterfeiting, corruption, and burglary theft and frauds, where major amounts are involved); and a miscellaneous group

87. Standing Committee on Justice and Legal Affairs, *Fourth Report* contained in Minutes and Proceedings of the Standing Committee on Justice and Legal Affairs No. 7, February 5, 1970, 2nd Session, 28th Parliament, No. 7:7.

88. See Appendix C.

89. R.S.C. 1970, c. 0-3, as amended.

(the supply, importation or exportation of controlled drugs, perversion of the course of justice, and blackmail).[90]

The emphasis throughout this guideline is on serious offences against individual or group well being — something not present in the offences listed in Part IV.I.

It is clear then that the proposals of the Standing Committee have not been implemented in the *Protection of Privacy Act*[91]. At present we have a lengthy list of crimes in Part IV.I as well as a wide definition of "Subversive activity" in the *Official Secrets Act*.[92] Accordingly, the scope of electronic surveillance under the present Act should be limited.

(b). *The Application Process*

The main concern with the application process in the present Act appears to be the unfairness of the *ex parte* application itself. This submission rests on the lack of procedural safeguards in both Part IV.I and the *Official Secrets Act*.[93] This reduces the controls on electronic surveillance that Parliament intended.

The nature of *ex parte* hearings themselves lend suspicion to possible abuses of due process since there is no third party representing the individual's interests. Under the *Official Secrets Act*[94] the sole authority for granting applications rests with the Solicitor General. Under Part IV.I fears of judicial rubber stamping have been justified by instances of application hearings taking only half an hour with some lasting less than fifteen minutes.[95]

The *Official Secrets Act*[96] is the worst of the amendments because it has virtually no safeguards at all. There is no provision that the application must be in writing, that there must be an accompanying affidavit, or that any other particulars must be stated. All that is required is that the Solicitor General be satisfied by evidence on oath that an interception is necessary for the security of Canada.

Similarly under Part IV.I there is the possibility of abuse of process. The McDonald Commission found instances of judge shopping.[97] The applicants would apply to a judge after they had been turned down by a different judge until they got the desired result. In the United States a system of random judicial rotation exists where the prosecutor is required

90. United Kingdom, *Report of the Royal Commission on Criminal Procedure* (1981) at 24.
91. S.C. 1973-74, c. 50.
92. R.S.C. 1970, c. 0-3.
93. *Id.*
94. *Id.*
95. McDonald Commission Second Report, vol. 2, at 1021.
96. R.S.C. 1970, c. 0-3, as amended.
97. McDonald Commission Second Report, vol. 2, at 1021.

to appear at a designated place and time to present his application. This method might reduce the possibility of judge shopping in Canada.

In either application hearing the interests of the individual are not represented. In Britain the Royal Commission on Criminal Procedure recommended that "the interests of the person subject to surveillance should be represented by the Official Solicitor or a similar body"[98]. This would be desireable in Canada and consistent with the intent of Parliament in maintaining safeguards for the individual.

(c). *Reviewing the Authorization Packet*

The inaccessibility of the authorization packet has raised concerns for the object of interception. Under s. 178.14 all documents related to the application are placed in a sealed packet and retained in a place to which the public has no access. The packet cannot be opened except for purposes of renewal or by order of a judge. This denies defence counsel the opportunity to see if there are any defects in the application documents.

Canadian case law suggests that the authorization packet is only accessible where there is extrinsic evidence to support an allegation of fraud or wilful non-disclosure.[99] This means that if a police officer was granted an authorization because he had stated in his affidavit that other investigative procedures had been tried when in fact they had not been, in absence of extrinsic evidence to prove this, defence counsel has no way of reviewing the application documents to show that the authorization was obtained by fraud.

Inaccessibility is not a concern to defence lawyers in the United States. Under Title III a copy of the authorization order along with the application documents must be furnished to both parties at least ten days prior to trial.[100] Such a provision would be desireable in Canada to ensure that there were no defects in the application documents.

(d). *Execution of Surveillance Orders*

Whether a police officer can enter the premises to install listening devices pursuant to an authorization order has been at issue for some time now. The matter has recently been decided by the Supreme Court of Canada.

At present the Canadian position seems to be that police can enter the premises without consent of the owner. In both *R.* v. *Lyons et al.*[101] and

98. *Supra,* note 90 at 39.
99. *R.* v. *Welsh (No. 6)* (1977), 32 C.C.C. (2d) 363 (Ont. C.A.).
100. Title III, s. 2518(9).
101. (1985), 56 N.R. 6 (S.C.C.).

the companion case *Interception of Private Communications Reference*[102] the Supreme Court of Canada held that Part IV.I does, by necessary implication, authorize trespass to carry out interceptions and that an authorization issued in the required terms includes authority to so trespass unless expressly prohibited in the authorization order. A resulting interception is therefore one which is "lawfully" made and communications received as a result of such interception are admissible as evidence. Presumably this would also apply to an authorization given under the *Official Secrets Act*.[103]

Prior to this the law was undecided in the area. The leading case on surreptitious entry was *R.* v. *Dass*[104] which held that an authorization order did not give police officers authority to enter a premises without consent in effecting an interception. Subsequent cases such as *R.* v. *Glesby et al*,[105] however, have held that Part IV.I gives an implied authority to enter the premises for the purpose of installing listening devices. The two conflicting views created uncertainty for lawyers, judges, police officers and individuals.

An additional concern during the *Dass* period was whether evidence obtained as a result of surreptitious entry was admissible. Under s. 178.16 of Part IV.I the interception must have been one which was lawfully made before it is admissible as evidence. The judge, however, has a discretionary power to admit evidence that would otherwise be inadmissible if it is relevant and is only inadmissible due to a defect in form or procedure in the application process.

In *Dass* the court held that a covert entry did not render the evidence inadmissible. An authorization made the interception one which was "lawfully" made within the meaning of s. 178.16. How the authorization was effected was only secondary to any evidence derived therefrom. The accused, however, still had a civil action against the police officers for trespass.

The only difference then between *Dass* and the recent Supreme Court of Canada decision is that the former allowed the accused a civil remedy against the police officers. Otherwise, there is no difference from the accused's point of view. On the one hand *Dass* said that the police cannot enter the premises while on the other hand it allowed evidence obtained through surreptitious entry. Thus, although the police did not have a right of entry any evidence obtained was admissible anyway. The Supreme Court of Canada merely took away the civil remedy by making covert entries legal.

102. (1985), 56 N.R. 43 (S.C.C.).
103. R.S.C. 1970, c. 0-3, as amended.
104. (1979), 8 C.R. (3d) 244 (Man. C.A.).
105. (1982), 2 C.R.R. 203, 19 Man. R. (2d) 438 (Co. Ct.).

The *Lyons*[106] case relied heavily on the American decision of *Dalia* v. *U.S.*[107]. In that case the Supreme Court of the United States analyzed the purpose and history of Title III and concluded that Congress intended to allow the courts to authorize electronic surveillance without limitations upon the means of effecting it. Accordingly, no specific authorization of surreptitious entry was required.

Although the Supreme Court of Canada did not consider the *Canadian Charter of Rights and Freedoms*[108] in its decision, Canadian cases may still follow American decisions which allow police to enter the premises in future *Charter* cases involving electronic surveillance. In *Dalia*[109] the American Fourth Amendment right against unreasonable search and seizure was considered yet it was not persuasive enough to convince the court against allowing covert entries to install listening devices. Similarly, *Glesby*[110] considered the right against unreasonable search and seizure guaranteed in s. 8 of the *Charter* but followed *Dalia.*

These are some of the difficulties with the present Act. It is suggested that the provisions discussed do not conform to the purpose and policies behind the Act. An effective balance between individual privacy and law enforcement has not been maintained. The prescriptions for change implicit in the *Charter* could put the scales back into place.

V. *Future Considerations*

1. *Charter Implications*

The provisions of the *Protection of Privacy Act*[111] clearly infringe upon the individual's right to privacy as well as the accused's right to a fair defence. The *Canadian Bill of Rights*[112] has not proved effective in rectifying the situation. In *Re Copeland and Adamson*[113] it was held that audio surveillance did not violate the due process clause because there is no common law right to privacy. Similarly in *R.* v. *Steinberg*[114] it was held that wiretapping did not contravene the right against self incrimination in s. 2(d) of the *Bill.* It is hoped that the *Canadian Charter of Rights and Freedoms*[115] will be useful in restoring the rights of the individual.

106. *Supra,* note 101.
107. 47 U.S. Law Week 4423 (1979); 441 U.S. 238.
108. See the *Constitution Act, 1982* [en. by the *Canada Act, 1982 (U.K.),* c. 11, Sched. B.], Pt. 1.
109. *Supra,* note 107.
110. *Supra,* note 105.
111. S.C. 1973-74, c. 50, as amended.
112. R.S.C. 1970, Appendix III.
113. *Supra,* note 12.
114. [1967] 1 O. R. 733 (C.A.).
115. *Supra,* note 108.

Since the *Protection of Privacy Act*[116] is largely an offspring of Title III, it is possible that future Canadian cases will revolve around the American decisions now that we too have a written Constitution. In the United States the constitutionality of electronic surveillance by law enforcement personnel has been dealt with on the basis of the Fourth Amendment right against unreasonable search and seizure. The Canadian counterpart can be found in s. 8 of the *Charter*.

The American decisions suggest that invasion of privacy is an important element in invoking the search and seizure provisions. Applying the Fourth Amendment in *Katz* v. *U.S.*[117] Mr. Justice Stewart stated that "what a person seeks to preserve as private, even in an area accessible to the public may be constitutionally protected".

Canadian *Charter* decisions on the other hand have been reluctant to include privacy as an element in electronic surveillance cases. In *R.* v. *Porter et al.*[118] it was held that surreptitious entry to install video equipment and the recording of images on video tape constitutes neither a search nor a seizure within the meaning of s. 8. The court was of the view that a seizure contemplates the forcible taking or holding of a person's possessions. It appears that privacy is not a possession capable of being seized.

Similarly in *R.* v. *Taylor*[119], surreptitious entry to install listening devices was held to constitute neither a search nor a seizure within the meaning of s. 8 nor did it offend the right to life, liberty and security of the person guaranteed in s. 7. The court held that the words search and seizure do not involve notions of privacy.

Although the Supreme Court of Canada specifically declined to comment on the *Charter* in *Lyons*[120] it did follow *Katz*[121] in an earlier search case. *Southam* v. *Hunter et al.*[122] was the subject of a search and seizure by the Combines Investigation Branch being held unreasonable within the meaning of s. 8. In that case the Supreme Court of Canada held that s. 8 is not restricted to the protection of property but rather guarantees a broad and general right to be secure from unreasonable search and seizure which includes a person's entitlement to a reasonable expectation of privacy. This could also apply to electronic surveillance.

What was an unreasonable search and seizure in *Southam*, however, may not be unreasonable in electronic surveillance cases. At issue in

116. S.C. 1973-73. c. 50, as amended.
117. 389 U.S. 347 at 354 (1967).
118. (January 17, 1983), 9 W.C.B. 311 (B.C. Co. Ct.).
119. B.C.S.C., December 30, 1983 (unreported).
120. *Supra*, note 101.
121. *Supra*, note 117.
122. (1985), 11 D.L.R. (4th) 641 (S.C.C.).

Southam was whether s. 10 of the *Combines Investigation Act*[123] allowing the Director of Investigation and Research, or his representative, to enter any premises and examine and take away documents relevant to matters being inquired into, was inconsistent with s. 8 of the *Charter* and therefore of no force and effect. In striking down the provision the Supreme Court of Canada held that the authorization procedure, which required only a certificate from a member of the Restrictive Trade Practices Commission, was incapable of being carried out in an entirely neutral and impartial manner and was therefore inconsistent with s. 8 of the *Charter.* In order to be consistent with the *Charter* the court held that the authorization procedure must be capable of being carried out in a judicial manner. The reasoning in *Southam* would not therefore be applicable under either Part IV.I or the *Canadian Intelligence Security Service Act*[124] since both require judicial authorization to conduct surveillance. The ability to act judicially might, however, be in question under the *Official Secrets Act*[125] which requires only the Solicitor General's authorization.

An additional concern under the *Charter* is whether assuming electronic surveillance is found to violate any guaranteed rights, it is nevertheless a reasonable limit within the meaning of s. 1. This section allows the state to violate a right or freedom if the infringement can be justified. Although the balance of interests involved was not addressed in *Southam*, the court did state that the onus of justifying a limitation upon a right or freedom lies with the party seeking to invoke the limit i.e. the state. Thus even if electronic surveillance was held to violate any rights under the *Charter* it could still be permitted by virtue of s. 1.

From the early decisions it appears that the *Charter* might not be useful in protecting the privacy of the individual in electronic surveillance cases. The Supreme Court of Canada just gave a green light to law enforcement agencies throughout Canada to use covert means in effecting surveillances. There is some hope however, with the notion of privacy being expressed in *Southam* as a constitutional right. The Supreme Court of Canada should take a liberal stance in invoking the *Charter* in future electronic surveillance cases. Failure to do so may bring the administration of justice into disrepute. We could soon see instances of police instigated crimes such as the John Delorean situation in the United States. These "pro-active policing"[126] techniques actually help effect the

123. R.S.C. 1970, c. C-23.
124. S.C. 1984, c. 21.
125. R.S.C. 1970, c. 0-3, as amended, s. 16.
126. Pro-active policing refers to acting before the crime is committed; Interview, Cpl. F. Baisley, Halifax Police Dept., (Nov. 1984).

crime. In such a situation this can hardly be called crime detection or law enforcement. Legislative change may well be needed to implant the balance between individual privacy and law enforcement that Parliament had in mind.

2. *Recommendations For Change*

To alleviate some of the defects that have been discussed, the McDonald Commission recommended several changes to the operation of the existing Act. To ensure an unbiased operation of the Act, they recommended the establishment of a National Review Commission, similar to the United States National Wiretap Commission, to oversee electronic surveillance by government agencies.[127] This Commission would be permitted access to the sealed authorization packets, as well as the intercepted communications, and could review the authorization documents in the application. The Commission would also sponsor, sessions in which judges from across the country meet and try to establish some standards by which the application documents should be considered. In addition, the Commission would prepare an annual report to Parliament, more detailed than presently required, assessing the performance of electronic surveillance in criminal investigations.

If such a Commission was established, it would at least ensure the reviewability of the authorization documents. However, it is not clear whether the proposed Commission would have the power to alter the authorization documents or invalidate the authorization should it have been obtained through fraud or wilful non-disclosure. This would be desireable in such a situation.

Further changes would have to be made in order to ensure minimal intrusion on individual privacy from government agencies. The list of offences in which electronic surveillance can be carried out should be limited. Instead of a lengthy list as in Part IV.I the emphasis should be on the seriousness of the offence with guidelines requiring the judge to take this into account. As well, the definition of subversive activity under the *Official Secrets Act*[128] should be more precise and allow less discretion to issue warrants than at present.

In the application hearings there should be some third party there to represent the interests of the object of interception. This would ensure that proper form and procedure are being followed and thus reduce the possibility of fraud or non-disclosure. In addition there should be an explanation of what information is required when applying for a warrant

---

127. McDonald Commission Second Report, vol. 2, at 1020.
128. R.S.C. 1970, c. 0-3, as amended.

under the *Official Secrets Act*[129] and the application process should be limited to designated agents only.

For applications under Part IV.I there should be a random rotation of judges thus eliminating the possibility of judge shopping.

In executing the authorization order surreptitious entry should not be allowed. At present the matter is not quite clear with one court saying the police cannot enter the premises and others saying they can. Parliament should make it clear that covert entries are not allowed. In addition, evidence obtained as a result of such an entry should be inadmissible.

These are some of the recommendations that would reduce intrusion into individual privacy by government agencies. There are of course other changes that could increase privacy rights, but short of abolishing the whole Act, these recommendations should deal effectively with the major concerns.

VI. *Conclusion*

The *Protection of Privacy Act*[130] sought to create a right to privacy, which before had not existed in Canada, by making it illegal to intercept private communications by means of electronic devices. It did, however, create exemptions from liability for the purposes of law enforcement. The Act therefore sought to maintain a balance of interests between individual privacy and law enforcement.

While the intent and purpose behind the Act seem agreeable, the provisions of the Act itself and the way they are being carried out clearly indicate that the Act favours police investigation more than individual privacy. This is evident from such things as the wide range of offences in which electronic surveillance can be used, the allowing of covert entries, the refusal to allow defence counsel to examine the authorization packets, the discretionary power given to the judge to allow evidence that would otherwise be inadmissible and a host of other items.

There does not seem to be much hope for change in the *Charter*, at least judging from the early decisions. Therefore it is clear that some legislative change will be needed. By following the recommendations suggested, in addition to any other changes Parliament would be willing to make, the privacy of the individual can be restored and the balance between individual privacy and law enforcement can be maintained.

---

129. *Id.*
130. S.C. 1973-74. c. 50, as amended.