CHAPTER 3

ELECTRONIC SURVEILLANCE — SECURITY SERVICE AND C.I.B.

A. ORIGINS, NATURE AND PURPOSE OF THE PRACTICE

1. The interception of telephonic messages has been technically possible since the early years of this century. In the United States, the constitutionality of the practice was argued before the Supreme Court in 1928[1] an indication of the rapidity with which law enforcement agencies recognized the potential worth of this technique. It has been used as an investigative technique by the R.C.M.P. since the 1930s. At the time counter-subversive functions were not performed by a branch separate from those in charge of criminal investigation, and there was nothing in the nature of counter-espionage being undertaken. Nevertheless, it was in what we would now regard as Security Service work that telephone tapping was begun in the latter part of that decade. In the years following the Second World War both telephone tapping and eavesdropping by means of microphones became more common among Canadian police forces. Telephones could be tapped by the installation of equipment along the telephone lines or at the telephone company's exchange. Later, telephone conversations could be listened to by means of induction devices installed in the telephone receiver; these were essentially the same for functional purposes as microphone "bugs" transmitting by radios which, with technical advances, could be installed more readily than the earlier microphones that transmitted by wire.

2. All these forms of eavesdropping devices were found to be valuable investigative techniques, both in the detection and investigation of crime and in the work of the Security Service. The increasing use of the technique by police forces received relatively little public attention in Canada. For the R.C.M.P. at least, telephone tapping was regarded as risky because it might involve violations of various statutes, and, to the extent that it was used at all, it was therefore regarded as an investigative aid to be employed in support of other techniques so that it would not have to be disclosed in court. Eavesdropping by microphone, so far as we can tell, was probably used more in Security Service

[1] (1928) 277 U.S.438.

functions (where the principal object is not the collection of evidence for the purpose of prosecution) than in criminal investigation, and in any event disclosure of its use in particular cases of criminal investigation would not have been regarded as a good idea because to do so would have alerted criminals and other adversaries to the techniques of installation and, in the particular case, might have exposed co-operating persons such as hotel employees and informers within criminal or subversive groups to the possibility of retaliation.

Criminal investigation

3. The value of telephone tapping in criminal investigation was testified to before us by Assistant Commissioner T.S. Venner, who, in 1973 became officer in charge of criminal intelligence for "O" Division (Southwestern Ontario):

> . . . when I came to "O" Division it was immediately apparent that, number one, it was virtually impossible to do effective criminal investigation in the City of Toronto, or in that general area, without telephone tapping on the criminal side. The difficulties that were presented by refraining from this activity were such that we were just almost out of business.
>
> (Vol. 33, p. 5440.)

The Annual Reports submitted by the Solicitor General of Canada reveal that in a significant number of criminal proceedings, evidence has been gathered from private communications intercepted pursuant to a judicial authorization issued under section 178.13(1) of the Criminal Code, and that a number of convictions have resulted. In numerous other cases information obtained from interceptions was used in the investigations though it was not offered in evidence.

	Cited as Evidence	"Used" but not in evidence	Convictions
1974 (half-year)	101	155	83
1975	395	879	246
1976	284	787	148
1977	198	546	134
1978	172	550	105
1979	101	155	83

This information is based on R.C.M.P. investigations, principally of offences under the Narcotic Control Act and the Food and Drugs Act, and conspiracy under the Criminal Code (most of which would no doubt be narcotic and drug cases).

4. The Annual Report for 1979, in its "General Assessment", disclosed the following statistics as to the first five years of the operation of the Protection of Privacy Act:[2]

	1974	1975	1976	1977	1978	1979
Authorizations granted	140(1)	562	613	615	712	764
Number of persons arrested	344	1561	1499	1213	1381	1177(2)
Number of convictions	238(3)	1125(3)	945(3)	680(3)	655(3)	225(3)
Authorization/Arrest ratio	2.5(4)	3.6(4)	2.5(4)	2.0(4)	1.9(4)	(6)
Arrest/Conviction ratio	69.2(5)	72.1(5)	63.0(5)	56.1(5)	47.4(5)	(6)

(1) Act in force for six months only in 1974.
(2) Other arrests pending.
(3) Cases are still before the courts in relation to investigations of authorizations originating in 1974 through to 1979.
(4) &(5) These ratios will increase as investigations and prosecutions are completed.
(6) No meaningful ratios available at this time.

Using 1975 as an example, the 1979 Annual Report showed that, allowing for the lapse in many cases of from one to at least four years between the granting of an authorization and arrests and convictions in the cases concerned, the figures originally reported in the year of the authorization undervalued the significance of electronic surveillance as an investigative technique. There were 562 authorizations in 1975. In those cases the following arrests and convictions ultimately occurred:

Results of 1975 Authorizations

	Number of Arrests	Number of Convictions
Figures reported in 1975	1,208	196
Figures amended in 1976	1,492	514
Figures amended in 1977	1,523	836
Figures amended in 1978	1,557	968
Figures amended in 1979	1,561	1,125

The Annual Report stated that at the end of 1979 there were still some cases concerning authorizations obtained in 1975 before the courts, so that the number of convictions is expected to increase slightly in 1980. This delay should be borne in mind in considering the apparently low number of cases in which evidence was adduced and convictions obtained in cases in which the

[2] The fourth and fifth categories of the table appear to be described incorrectly: the fourth category should be "Arrest/authorization ratio", and the fifth category should be "Conviction/arrest" and is, it should be observed, not a ratio but a percentage.

authorizations were granted in the years 1976 to 1979: the full story of the number of convictions obtained in those cases is not yet known.

5. It is important to note that the statistics shown here relate to applications for authorizations made by agents of the Solicitor General of Canada, and do not include any information concerning applications made by agents of provincial attorneys general. The latter would cover the majority of investigations under the Criminal Code. Thus, for example, the Annual Report of the Attorney General of Ontario for 1978 disclosed that in that year in Ontario there had been 237 applications for authorizations for wiretapping. In 1978 these applications in Ontario covered the following offences:

	Suspected Substantive Offence	Suspected Conspiracy to Commit the Offence
Bookmaking	61	45
Theft, robbery and breaking and entering to commit theft	52	47
Possession of stolen property	41	36
Fraud	32	31
Murder	26	18
Extortion	20	19
Possession of counterfeit money	10	0
Forcible confinement	5	0

Although those figures are not related to investigations conducted by the R.C.M.P., the overall purpose of electronic surveillance cannot be understood without reference to the provincial scene. Of particular interest is the fact that the 1978 Annual Report of the Ontario Attorney General disclosed that 76 transmitting devices were installed. Although no precise information is available, it may reasonably be inferred that a number of such microphone installations by police forces other than the R.C.M.P. have been made by entry without the consent of the person entitled to give permission to enter the premises. Thus the legal problems in Chapter 2 of this Part are not limited to the work of the R.C.M.P.

Security Service

6. From July 1, 1974, to the present, most warrants signed by the Solicitor General have been signed by him at his regular weekly meetings with the Director General. The totals of warrants issued from 1974 to 1978 inclusive have been stated in the Annual Reports made by the Solicitor General to Parliament pursuant to section 16(5) of the Official Secrets Act, as follows:

1974 — 339
1975 — 465
1976 — 517
1977 — 471
1978 — 392
1979 — 299

7. The annual figures are somewhat misleading because they include renewals which, in December of each year from 1974 to 1978, were signed by the Solicitor General to authorize continuation, from the first day of the following January until the 31st day of the next December, of the interception of communications under warrants already signed. This procedure is not provided for by the statute. It resulted from an administrative decision made within the Security Service that all warrants should be issued for periods no greater than the period ending December 31 of the year in which the warrants are issued. This decision was made by the Security Service with good intentions, as it was thought that otherwise the statistics provided to Parliament would be misleading in that, if a warrant were granted for a period expiring in the following year, the annual report to Parliament would not in fact disclose the total number of warrants which were in effect in that year. However, it does not seem to have been realized that the new system led inadvertently to another misinterpretation.

8. There is no provision in section 16 of the Official Secrets Act for renewals of warrants. By way of contrast, section 178.13(3) of the Criminal Code expressly provides that a judge may grant "renewals of an authorization" from time to time. The Honourable Allan Lawrence, Solicitor General in December 1979, did not follow the procedure which his predecessors had followed. Perhaps this was because the issue of the validity of the granting of renewals had been raised with Mr. Allmand during the latter's *in camera* testimony on December 3, 1979, later made public in Vol. 162 (March 7, 1980). The procedure followed by Mr. Lawrence was to receive applications for new warrants only.

9. The renewal procedure and its effect on the statistics are exemplified by the fact that on December 20, 1974, Mr. Allmand signed a document purporting to renew 222 warrants previously granted by him. The number of warrants reported in the Annual Report for 1975 as having been issued in 1975 included the 222 renewals. The same was true in following years. Thus in December 1975, there were 214 renewals, of which 128 were renewals of warrants which had originally been granted in 1974 and renewed in December 1974. On December 20, 1976, 199 renewals were granted, of which 97 referred to warrants originally granted in 1974 and renewed at the end of both 1974 and 1975, and 28 referred to warrants which had been issued in 1975 and renewed at the end of 1975.

10. It should not be assumed that the Solicitors General have acted as rubber stamps upon receipt of applications for warrants. Eleven applications made to the various Solicitors General from 1974 to 1978 inclusive were refused. One Solicitor General rejected three applications but subsequently granted them when more information, especially as to the likelihood of the usefulness of the warrant, was provided to him. Another rejected three applications, one because it was proposed to be used to intercept the communications of a person on a university campus, a second for a reason that was not recorded by the Security Service, and a third for the reason, as reported on Security Service files, that he knew one of the people in the suspect group and was sure that that person was doing nothing illegal. (That former Minister, however, has told us that he remembers the application and that that is not what he said. He says that he

did not know the person but had heard of him, and that he did not say he was sure that the person was doing nothing illegal. What he did say, according to the Minister, is that he needed better evidence that the group fell within the statutory provisions.) Another Solicitor General rejected five applications. One of these applications had been made on the ground that the target was said to be a member of a foreign terrorist group and who had participated in a bank robbery in his native country in an attempt to collect funds for the terrorist group. In one instance the Solicitor General rejected the application because he required more information that the person was involved in the terrorist field "in Canada". Later in this chapter we shall comment on whether the statute requires such proof; our point here is simply that the Solicitor General did not grant the warrant sought.

11. The previous paragraph affords substantial evidence that the Solicitors General did not always comply with the wishes of the Security Service as expressed in applications made under section 16(2). In this regard the following points should also be noted. Three warrants, which had been issued and acted upon were subsequently terminated by the Solicitor General contrary to the wishes of the Security Service. Three warrants issued by the Solicitor General were for a shorter period than the Security Service had requested, and were not renewed at the expiry of the period. Finally, on one occasion, a Solicitor General, in a special review requested by him of 22 warrants, cancelled six of them, as in his opinion their continuation was not justified.

B. R.C.M.P. POLICIES CONCERNING THE PRACTICE

Criminal Investigation Branch

12. In those parts of Canada served by the Bell Telephone Company, it was an offence, even before July 1974 when wiretapping was not covered in the Criminal Code, to intercept wilfully any message transmitted on the company's telephone lines. Section 25 of the Act incorporating the Bell Telephone Company of Canada reads as follows:

> 25. Any person who shall wilfully or maliciously injure, molest or destroy any of the lines, posts or other material or property of the company or in any way wilfully obstruct or interfere with the working of the said telephone lines or intercept any message transmitted thereon shall be guilty of a misdemeanour.[3]

13. This section does not appear to have been interpreted in any court until the decision in *Re Copeland and Adamson* in 1972. Mr. Justice Grant held that telephone tapping was not a violation of the section:

> The only part of such section which it might be said would be breached by wire-tapping would be the words "interfere" or "intercept". Can it be said that listening in on a telephone conversation is properly described by either of such terms? The Shorter Oxford English Dictionary defines the word "interfere" as follows:
>
> "To interpose — intersperse; to strike against each other; to come into collision; to exercise reciprocal action so as to increase, diminish or nullify the natural effects of each."

[3] S.C. 1880, ch.67, s.25.

It defines the word "intercept" as follows:

> "To take or seize by the way or before arrival at a destined place; to stop or interrupt the progress or course of; to interrupt communications or connections with."
>
> I do not believe that wire-tapping which does not impede the conversation between the parties nor impede its progress can form a breach of such section because the material before me does not indicate that the audio surveillance creates any disturbance of the conversation.[4]

The same point of view was expressed by a brief on wire-tapping prepared in 1965, apparently by the Legal Branch of the R.C.M.P., which pointed out that the phrase "intercept any message", in the absence of judicial interpretation, "must take its everyday meaning, i.e. to take or seize on the way from one place to another, cut off, check, stop — in other words so that the message would not be received by the intended receiver." However, it may be assumed from what follows that, before *Re Copeland and Adamson* was decided, at least some people thought that the word "intercept" included listening. (It may be noted that section 178 of the Criminal Code, which came into effect on July 1, 1974, has specifically avoided the difficulty by defining "intercept" as including "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof".)

14. In two provinces, Alberta and Manitoba, legislation specifically prohibited the interception and clandestine recording of telephone messages by any means, including induction, as Commissioner McClellan noted in a letter to the Deputy Minister of Justice in 1965. The Commissioner, probably relying on the legal brief, did not mention the provision in the Bell Telephone Act in his letter. He wrote that

> . . . with the exception of the Provinces of Manitoba and Alberta, there is no legislation in force primarily enacted to prohibit telephone intrusion.

He expressed his "belief that a law enforcement agency is not prohibited from intercepting telephone conversations". (Ex. E-1, Tab 21).

15. In 1936 it appears that Assistant Commissioner G.L. Jennings, who was Director of Criminal Investigation, consulted the Deputy Minister of Justice with regard to wiretapping. A member of the Department prepared a memorandum of which a copy was then sent by the Deputy Minister to Assistant Commissioner Jennings. The memorandum quoted section 25 of the Bell Telephone Act, then, clearly assuming the practice to be illegal, cited three Canadian judicial decisions that evidence is admissible in court even if obtained illegally. Assistant Commissioner Jennings in his acknowledgement to the Deputy Minister, described the memorandum as including "legal opinions on the admissibility of evidence obtained in an irregular manner" and advised that the information had been disseminated throughout the Force. In his letter to the officers commanding the various divisions the Assistant Commissioner observed that it might be necessary to resort more and more to wiretapping, and that "the consensus of the legal opinion" is that evidence obtained "in an

[4] [1972] 3 O.R.248, 28 D.L.R. (3d) 26.

irregular manner" is admissible and that it is "not material to the case in what manner such evidence was obtained". (Ex. E-1, Tab 1A.)

16. Thus R.C.M.P. Headquarters encouraged the use in some of its Divisions of a technique that was then thought to be an offence under the Bell Telephone Act. Presumably wiretapping was used in criminal investigations at least until 1959, for in March of that year a memorandum by Inspector (later Commissioner) Higgitt recorded that Commissioner Nicholson had "forbidden the use of technical aids equipment for the interception of telephone conversations". (Ex. E-1, Tab 1B.)

17. From that time onward there is considerable evidence (Ex. E-1, Tab 2) that senior officers at Headquarters, including Commissioner Lindsay in 1967 and three Directors of Criminal Investigation in 1964, 1966 and 1969, reiterated the policy forbidding the use of telephone tapping by members of the Force in the investigation of criminal matters. Indeed, in 1966 Commissioner McClellan, in a letter, assured the Solicitor General, the Honourable L.T. Pennell, "that this Force does not practise telephone tapping in the investigation of criminal matters". (Ex. E-1, Tab 2K.) At a meeting on July 5, 1968, according to a memorandum prepared by Commissioner Lindsay, he and other senior officers advised the Solicitor General, the Honourable John N. Turner, of "the total absence of wiretapping by us in this field" (i.e. in criminal investigations). A note from Commissioner Lindsay records that the same matter was discussed "in general terms" on July 11, 1968, with the newly appointed Solicitor General, the Honourable George McIlraith. An exception was made in cases where the consent of one of the parties to the conversation was obtained. At the time the listening and recording of a conversation with the consent of one of the parties was done by using an induction device near but not necessarily attached to the party's telephone or wire. Even this technique was not permitted in Alberta and Manitoba, because of local legislation (Vol. 33, pp. 5430-1). This technique might have been a violation of section 25 of the Bell Telephone Act, but the practice was known in the courts and even by Chief Justice Dorion (in the Inquiry into the Munsinger affair in 1965) without raising adverse comment. Nevertheless, these senior R.C.M.P. officers wanted the use of this investigative aid to be kept out of the public eye as much as possible, particularly as they had hopes of obtaining legislation that would permit the use of wiretapping by warrant, and they feared that public exposure might prejudice the enactment of the legislation. Although the Force's policy forbade participation in joint operations with other Canadian police forces in the interception of telephone messages or in manning listening posts, there was no hesitation in using the product of such activities or transcribing tapes. In fact, the prohibition of telephone taps by Headquarters was seen by the Force to cause tensions with other police forces, most of which conducted telephone tapping (Vol. 33, pp. 5395 and 5400).

18. Therefore, so far as can now be ascertained, and so far as practice reflected Headquarters policy, the use by the R.C.M.P. of devices to intercept telephone conversations, at least from 1959, was limited to the use of induction devices with the consent of one party to the conversation. According to *Re Copeland and Adamson*, however, this was not an offence.

19. It is clear that the policy enunciated by Headquarters, and the assurances given so positively to government that telephonic interception was not permitted, were somewhat meaningless. Assistant Commissioner T.S. Venner testified that in "some areas" R.C.M.P. investigators "simply relied on their local, municipal and provincial police counterparts to do this work for them". In other areas,

> ... our policy was held to be just a guideline, and key personnel, when operational circumstances warranted it, went ahead with the necessary activity, either not reporting it at all, reporting it only up to certain levels or reporting it in an incomplete, less than fully informative fashion.
>
> (Vol. 33, p. 5404.)

One such area was "O" Division (Southwestern Ontario), to which Mr. Venner was transferred from Edmonton in the summer of 1973. Put more bluntly by him, the fact that telephone tapping was being carried on in the field was "withheld" from senior officers of the Force who were responsible for the policy and were assuring Parliamentary Committees that there was no wiretapping for criminal investigation purposes (Vol. 33, p. 5453). Indeed, in those areas where the policy was ignored in practice, the R.C.M.P. now recognizes that the telephone tapping was "carried on in an atmosphere of non-accountability, fear of discovery, even deception" (Vol. 33, p. 5407).

20. Mr. Venner told us that when he moved from Alberta to Toronto in 1973 as Officer in Charge of the Criminal Intelligence Division

> It also became apparent that telephone tapping was going on, was being conducted by our criminal investigators, and to a very high degree it also became apparent that this was an underground activity, that it was not being reported, that information as to the character and extent of our technical activity was being withheld from superior officers, and the people who were doing it were people who became immediately subordinate to me as soon as I arrived there.
>
> (Vol. 33, p. 5440.)

So, after examining the situation, he concluded that it was "impractical" not to tap telephones, "policy notwithstanding". Although it was "clear" to Assistant Commissioner Venner that in 1973 "it was still a policy of the Force not to wiretap" (Vol. 33, p. 5454), he considered the policy to be

> ... a guideline to be followed wherever possible, but when it was just not practical to live within that policy, and where there was a greater public interest, in my assessment, at stake, then telephone intrusion would form part of our electronic surveillance program.
>
> (Vol. 33, p. 5441.)

He was aware not only that the practice was contrary to Force policy, but that, in the small percentage of cases in which it was necessary to enter premises in order to tap a telephone, there was ("at most") a violation of the Ontario Petty Trespass Act and possibly civil trespass (Vol. 33, pp. 5441-44).

21. This attitude was not restricted to Southwestern Ontario. In a letter to the Solicitor General on October 6, 1977, Commissioner Simmonds wrote

> Efforts to have our policy changed met with no success for a variety of reasons and it became evident that there was a wide range of interpretation

being applied with respect to the prohibition against telephone tapping. In some areas, our investigators simply relied on their local, municipal and provincial police counterparts to do this work for them. In other areas, our policy was held to be just a guideline, and, key personnel, when operational circumstances warranted it, went ahead with the necessary activity either not reporting it at all, reporting it only up to certain levels or reporting it in an incomplete, less than fully informative fashion. In some other areas, the policy was rigidly adhered to, occasionally because local enforcement programs were sufficient without this investigative aid, but more often because the policy and public pronouncements by the Commissioners where held to be an absolute bar to telephone tapping in the investigation of criminal matters. I think it is fair to say that where this interpretation existed and was applied, telephone tapping simply continued in an "underground" fashion and our previously high standards of accountability became subject to violation. The damage this did has not yet been fully repaired.

(Ex. E-1, Tab 1.)

22. The self-imposed limitation was removed with the enactment of the Protection of Privacy Act, which came into effect on July 1, 1974. At least as far as the R.C.M.P. was concerned, that Act has apparently vastly increased the use of telephone intercepts for criminal investigation purposes.

Security Service

23. The R.C.M.P. Security Service has been intercepting telephonic communications since arrangements were completed for that purpose in 1951, under the Emergency Powers Act, which empowered the Minister of Justice to require a communications agency to produce or make available, any communication "that may be prejudicial to or may be used for purposes that are prejudicial to the security or defence of Canada". Superintendent George McClellan, who was then officer in charge of Special Branch, expressed the view, in a memorandum for the Honourable L.B. Pearson, that there was no legislation barring such action. However, the Minister of Justice, the Honourable Stuart Garson, appears to have been of a different view in January 1951 and a special procedure was apparently adopted to resolve the problem.

24. The Emergency Powers Act expired on May 31, 1954. That month the R.C.M.P. proposed that sections 3 and 11(1) of the Official Secrets Act could provide a satisfactory authority for continuation of interceptions of telephone communications after that date. On June 16, 1954, the Deputy Minister of Justice, Mr. F.P. Varcoe, gave a written opinion to the Minister of Justice, which for the next 20 years was known as "the Varcoe opinion" and was the rationale for the interception of telephonic communications for security purposes. His opinion was that telephonic communications could be intercepted pursuant to a search warrant granted by a justice of the peace under section 11(1) of the Official Secrets Act.

25. At the date of that opinion the relevant provisions of the Official Secrets Act[5] were as follows:

> 3. (1) Every person who, for any purpose prejudicial to the safety or interests of the State, (c)... communicates to any other person any... in-

[5] R.S.C. 1952, ch.198.

formation that is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power; is guilty of an offence under this Act.

11.(1) If a justice of the peace is satisfied by information on oath that there is reasonable ground for suspecting that an offence under this Act has been or is about to be committed, he may grant a search warrant authorizing any constable named therein, to enter at any time any premises or place named in the warrant, if necessary by force, and to search the premises or place and every person found therein, and to seize any sketch, plan, model, article, note or document, or anything that is evidence of an offence under this Act having been or being about to be committed, that he may find on the premises or place or on any such person, and with regard to or in connection with which he has reasonable ground for suspecting that an offence under this Act has been or is about to be committed.

The reasoning, in part, was that while the search warrant provision in the Criminal Code is open to the possible construction that it relates only to tangible evidence, section 11 of the Official Secrets Act extends to "anything that is evidence of an offence under this Act". This "anything" must include oral communications, since the communication of information of the kind referred to in section 3, and in the circumstances referred to in that section, constitutes an offence, and Parliament must be presumed, in enacting section 11, to have had in mind every means of communication, including telephonic communication. Mr. Varcoe recommended a form of search warrant that was to be granted by a justice of the peace, reading as follows:

OFFICIAL SECRETS ACT

WARRANT TO SEARCH

Canada,
Province of ,
City of ,

To.....of the Royal Canadian Mounted Police in the said City of .....

WHEREAS it appears on the oath of..... that there are reasonable grounds for suspecting that an offence under the Official Secrets Act has been or is about to be committed, to wit: that information that is calculated to be, might be, or is intended to be, directly or indirectly useful to a foreign power concerning secret official code words, pass words, sketches, plans, models, articles, notes or other documents, prohibited places or things in prohibited places, or concerning things made or obtained in contravention of the Official Secrets Act, has been or is about to be published, communicated or transmitted by means of the telephone installed in .....

(here describe location of phone i.e. "house bearing civic number-..... street"
or
"apartment (or suite) no..... in the building bearing civic number-..... street" but do not use word "premises")

to agents of foreign powers and to other persons not lawfully entitled to receive such information, for purposes prejudicial to the safety or interests of the State; and that there are reasonable grounds for suspecting that evidence or communications that are evidence of an offence under the Official Secrets Act having been or about to be committed, by the communication, publication or transmission of such information by means of the said telephone, may be found in the premises of . . . . (hereinafter called the premises);

This is therefore to authorize and require you to enter into the said premises at any time and to search for, seize and record any communication or communications transmitted by means of said telephone installed in . . . . that is or are evidence of an offence under the Official Secrets Act having been or being about to be committed and with regard to or in connection with which you have reasonable ground for suspecting that an offence under the said Act has been or is about to be committed.

Dated this . . . . day of . . . . A.D., 195...

.....

Justice of the Peace in

and for . . . .

The intention of the R.C.M.P. in suggesting this procedure was to rely on section 17(1) and (2) of the R.C.M.P. Act which makes the Commissioner and every Deputy Commissioner, Assistant Commissioner, Chief Superintendent and Superintendent *ex officio* a justice of the peace. This procedure was in fact followed from 1954 onward. However, ten years later, the Minister of Justice, the Honourable Guy Favreau, by letter dated September 4, 1964, imposed a control mechanism which required the Commissioner to seek the authorization of the Minister in writing before the Commissioner (acting as a justice of the peace) would issue such a search warrant. The Commissioner was to make a written request for such authority to the Minister, who was to be satisfied "that such facilities are being or are likely to be used by a person engaged in, or reasonably suspected by the Commissioner of being engaged in or about to engage in activities which constitute offences made under the Official Secrets Act". There was an emergency provision for the Commissioner to issue a warrant for 72 hours. The Minister was to carry out a monthly review of all outstanding search warrants and he might re-authorize those which, in his opinion, there were sufficient grounds to retain. The interception of telegraphic communications was, as previously, to be based on an Order of the Minister of Justice under the authority of section 7 of the Official Secrets Act.

26. It was on the basis of the "Favreau letter" that the Ministers responsible for the R.C.M.P., until June 1974 received and approved monthly "certificates of review" for all current warrants for the interception of telephonic communications.

27. It should be noted that this procedure did not cover the interception of oral communications by microphone. The reason for the procedure in respect of telephonic communications was that the telephone companies wanted a legal

basis for the co-operation they were being asked to extend. No such concern inhibited microphone operations.

28. The Security Service policies concerning electronic surveillance by "bugging" — i.e. microphone installations — have been reviewed in Chapter 2, section B, because the legal issues arising from that practice relate to "Surreptitious Entries" and were best discussed under that heading.

29. Two examples might be useful in illustrating that the Security Service at Headquarters has exercised some prudence in deciding whether to apply for warrants. In one instance, the person whose communications were the subject of a proposed application for a warrant was an executive member of an organization about which Headquarters decided not to make application because the activities were not considered to be subversive. In the other instance, the targetted group had its origins in another country and a history of terrorist acts in Canada and other countries. While an earlier warrant had been granted against members of the group in Canada, a subsequent request by the field unit that a warrant be applied for in respect of the communications of a person believed to be the leader of the group in Canada was turned down by Headquarters because Headquarters had learned that the reason for the group's violent activities had ceased to exist.

C. EXTENT AND PREVALENCE — SECURITY SERVICE AND C.I.B.

(i) *Security Service*

30. Before July 1, 1974, as has already been indicated, "wiretapping" (which includes the interception of both telephone conversations and telex messages) was a common and frequently used investigative technique throughout Canada — and consequently in those provinces where it may have been an offence. The use of microphone installations, which *per se* was not unlawful but gave rise to legal issues in regard to the *manner* of their installation, use and removal, was also general and frequent.

31. Since July 1, 1974, the legal issues in regard to both wiretapping and microphone installations have changed. The use of both techniques remains general and frequent, and is disclosed in the Annual Reports of the Solicitor General.

(ii) *Criminal Investigation Branch*

32. We have already described the official refusal of the Force to permit the use of telephone tapping before July 1, 1974, and we have described what evidence we have obtained of the policy being disregarded at the local level. The evidence tended to refer to telephone tapping, and there is no evidence before us as to the use of microphones, but the extensive use of the latter since July 1, 1974, would lead us to infer that the evidence we received, which was expressed in terms of telephone tapping, applied equally to other forms of electronic surveillance.

33. Since July 1, 1974, the extent to which those techniques are used by the R.C.M.P. and other police forces has been disclosed in the Annual Reports of the Solicitor General of Canada and the attorneys general of the provinces which have been referred to in section A of this Chapter. They are used very extensively in the investigation of crime.

D. LEGAL AND POLICY ISSUES

(a) *Legal issues common to Security Service and C.I.B.*

Violations of Provincial Statutes

34. We have already described the most significant legal issue regarding telephone tapping before July 1, 1974. That issue was whether it constituted an offence under section 25 of the Bell Telephone Act. In *Re Copeland and Adamson* it was held not to be an offence under that Act unless the conversation was disturbed by the eavesdropping. Legislation in certain provinces also requires consideration in deciding whether telephone tapping before July 1, 1974, constituted an offence. The Alberta Government Telephone Act[6] makes it an offence to interfere with the provincial equipment or facilities, record conversations without advising the other party in advance and to use profane and other specified language on a telephone or telecommunication wire. The Manitoba Telephone Act[7] deals with the connection of receiving and transmitting equipment to provincial facilities without the approval of the Provincial Commission. The Act also prohibits the recording of telephone conversations in Manitoba unless the other party to the conversation is properly advised of the proposed recording. The Nova Scotia Rural Telephone Act[8] provides penalties for wilful and malicious interference with provincial telephone company equipment. The Quebec Telegraph and Telephone Companies Act[9] prohibits the use of provincial equipment to acquire, without lawful authority, knowledge of private conversations.

35. The Telephone Act of Ontario[10] prohibits interference with equipment and the divulging of telephone conversations to persons who were not parties to a conversation except when lawfully authorized or directed to do so. The Ontario Legislation was held to be *intra vires* the province: *R.* v. *Chapman and Grange.*[11] These provincial legislative provisions under which offences may, at least before July 1, 1974, have been committed by members of the R.C.M.P. engaged in the investigation of crime, do not appear to have been considered at any time within the R.C.M.P. when deciding upon the policy in regard to telephone tapping.

---

[6] R.S.A. 1970, ch.12.
[7] R.S.M. 1970, ch.T-40 as amended by 1977 Man., ch.45.
[8] R.S.N.S. 1963, ch.273.
[9] R.S.Q. 1964, ch.286.
[10] R.S.O. 1970, ch.457.
[11] [1973] 2 O.R. 290.

36. These provincial statutes continue in effect. However, it is likely, in our view, that the entry of the Parliament of Canada into the field by the enactment of the Protection of Privacy Act means that the provincial legislative provisions are no longer effective in so far as they are in respect of the same forms of conduct as are covered by the criminal legislation. Therefore it is likely that, since July 1, 1974, when members of the R.C.M.P. have tapped telephones under an authorization by a judge under section 178 of the Criminal Code or by the Solicitor General under section 16 of the Official Secrets Act there has been no offence committed under provincial legislation.

37. As for the Security Service, the position since 1974 has just been referred to. Before July 1, 1974, the tapping of telephones was carried out pursuant to warrants issued under section 11 of the Official Secrets Act. Consequently it is unlikely that offences were committed under the provincial statutes.

38. Listening to telephone communications in British Columbia and Saskatchewan (which do not have statutes creating offences specifically in regard to telephones) and *all* forms of electronic surveillance in those provinces as well as Manitoba may violate the provisions of the Privacy Acts of those provinces.[12] These statutes create "a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another".[13] With minor differences the three provincial statutes very closely resemble each other. All three provide that privacy may be violated by eavesdropping or surveillance whether or not accomplished by trespass. However, they all provide certain defences to such actions, one of which is particularly pertinent. As stated in the Saskatchewan Act (and similarly in the statutes of the other provinces):

> 4. (1) An act, conduct or publication is not a violation of privacy where:
>
> (a) it is consented to, either expressly or impliedly by some person entitled to consent thereto;
>
> ...
>
> (c) it was authorized or required by or under a law in force in the province or by a court or any process of a court; or
>
> (d) it was that of:
>
> (i) a peace officer acting in the course and within the scope of his duty; or
>
> (ii) a public officer engaged in an investigation in the course and within the scope of his duty;
>
> and was neither disproportionate to the gravity of the matter subject to investigation nor committed in the course of trespass.

In the case of defences for peace and public officers the Acts seem to set up a series of variable permissible violations of privacy directly proportionate to the seriousness of the "crime".

---

[12] Stats. B.C. 1968, c.39; Stats. Saskatchewan 1973-74, ch.80; Stats. Manitoba 1970, ch.74.

[13] Privacy Act, Stats. B.C. 1968, ch.39, s.2(1).

39. However, if a policeman cannot be said to be carrying out his duty if he violates some other law, such as the law of trespass, the general applicability of a defence under section 4(d) must be discounted in cases of surreptitious entry. On the other hand authorizations or warrants issued since July 1, 1974, under section 178 of the Criminal Code or section 16 of the Official Secrets Act would mean that most otherwise actionable incidents involving members of the R.C.M.P. would be covered by a defence under section 4(c).

40. We turn now to a consideration of a number of legal issues which are common to both sides of the Force and pertain to the period from July 1, 1974, to the present time.

Entry into private premises

41. The first issue to be considered is whether a judge or a Solicitor General, in issuing a warrant, has the statutory power to authorize entries to install, repair and remove a listening device, and whether if he does not expressly do so, the power is implied. During the early months of 1972, while consideration was being given in government to the Protection of Privacy Bill, the R.C.M.P. suggested to the Department of Justice that it was preferable that even in criminal investigations the legislation should provide for authorizations by the Solicitor General of Canada or by provincial attorneys general rather than by judges. The reason given by the R.C.M.P. was that a judge might refuse to grant an authorization to plant a listening device if he were aware that "unorthodox investigative methods" must be employed. It was also suggested that the legislation should contain a specific power to install the device, including the power to make surreptitious entries. This, it was suggested, would be in keeping with the recommendations of the Report of the Canadian Committee on Corrections, 1969, which said that ". . . police powers should be clearly defined and readily accessible". The R.C.M.P. considered that such an express statutory power of entry was necessary despite the existence of subsection 26(2) of the Interpretation Act.[14] Some doubt was expressed as to whether this subsection could be relied upon in these circumstances.

42. Following this, memos were exchanged among various R.C.M.P. and government officials as a result of a suggestion that had been made to the effect that specific provisions authorizing entry were necessary in the proposed legislation dealing with telephone interception both in the Official Secrets Act and the Criminal Code. On April 19, 1972, Mr. Starnes, Director General of the Security Service of the R.C.M.P., in a letter to Mr. Goyer, agreed that the legislation should provide specific provisions for entry upon "telephone company premises, installations, and dwellings generally". Mr. Starnes felt that these provisions should also exempt telephone company employees from liability when acting in good faith and under the direction of a peace officer. Mr. Goyer in turn wrote the Honourable O.E. Lang, then Minister of Justice, to the same effect. Mr. Lang, in reply, assured Mr. Goyer that a peace officer performing his duty under the proposed legislation would have authority to enter premises. He felt that the presence of section 26(2) of the Interpretation

[14] R.S.C. 1970, ch.I-23.

Act was sufficient to cover this matter and therefore there was no need to be specific on this point in the proposed legislation. Consequently no such express power to install, or to enter premises to install (or to enter premises to conduct a survey before the application, or to repair or maintain the device, or to remove it) was included in the legislation, either in respect of interceptions made pursuant to judicial authorizations or those made pursuant to a Solicitor General's warrant.

43. In order to understand this decision it is necessary to cite the relevant provisions of the Interpretation Act and section 25(1) of the Criminal Code:

Interpretation Act:

> 3. (1) Every provision of this Act extends and applies, unless a contrary intention appears, to every enactment, whether enacted before or after the commencement of this Act.
>
> 26. (2) Where power is given to a person, officer or functionary, to do or enforce the doing of any act or thing, all such powers shall be deemed to be also given as are necessary to enable the person, officer or functionary to do or enforce the doing of the act or thing.

Criminal Code:

> 25. (1) Everyone who... is authorized by law to do anything in the administration and enforcement of the law
>
> (b) as a peace officer... is, if he acts on reasonable and probable grounds, justified in doing what he is required or authorized to do and in using as much force as is necessary for that purpose.

44. According to the testimony of Assistant Commissioner T.S. Venner, an oral opinion was given by the Department of Justice to the R.C.M.P. in May 1974, the purport of which was shared by the Legal Branch of the R.C.M.P. This opinion, given before the Protection of Privacy Act came into effect in July 1974, was to the effect that authorizations under the new legislation did not expressly allow for entry into premises, and that the Force would have to rely on section 26(2) of the Interpretation Act and section 25(1) of the Criminal Code to justify such operations. A Legal Branch memorandum dated April 29, 1974, reported on a meeting with Mr. Scollin and Mr. D.H. Christie, Associate Deputy Minister of Justice, at which, according to the memorandum, it was agreed that a sound basis in law for the use of surreptitious entries under the new provisions of the Official Secrets Act was to be found in section 26 of the Interpretation Act.

45. On July 8, 1977, Mr. Louis-Philippe Landry, who was then Assistant Deputy Attorney General, wrote to the Deputy Solicitor General, Mr. Tassé, concerning "allegations of break-ins by members of the R.C.M.P. for the purpose of installing electronic listening devices", which had apparently been discussed recently by them. (Ex. E-1, Tab 2G.) With regard to entries made since July 1, 1974, when an authorization has been issued by a judge pursuant to section 178.13, he wrote:

> When a judge authorizes a peace officer to intercept private communications, the peace officer may, in order to achieve that purpose, enter

> premises in order to install the required electronic devices without the knowledge of the occupant or owner of such premises. I understand that most authorizations given provide for the authorization to enter premises for such purposes. However, even in a case where the judge's authorization is not a specific authorization to enter premises for such a purpose, the officer who installs an electronic listening device for the purpose mentioned in the authorization is not breaking any law.

(As will be seen, we have doubt that, where the authorization was for a listening device, most judges would include an express authorization to enter premises for such purposes. However, conclusive research is impossible because of the statutory provisions against disclosure.)

46. On July 21, 1977, the officer in charge of the Legal Branch argued in a memorandum that, even if section 26(2) of the Interpretation Act and section 25(1) of the Criminal Code gave the implied power to enter to make an installation, it is doubtful that they give the implied power to enter to remove it. However, on November 4, 1977, he wrote to Mr. Landry expressing the view that an authorization of interception implicitly allows the police to remove the device, even after the period stated in the authorization has expired. The Director of the Criminal Law Section of the Department of Justice replied on November 9, 1977, agreeing with that conclusion on the ground that "since the Order authorizes the interception of communications during a specific period of time, it is implicit that the device must be allowed to remain until that time expires".

47. On September 22, 1977, Commissioner Simmonds sent messages to the field directing that no surreptitious entry was to take place to install electronic surveillance equipment unless the words "to install, monitor and remove" are in the authorization received under the Protection of Privacy Act (Ex. E-1, Tab 3G).

48. On June 9, 1978, Mr. Landry wrote letters to all the provincial attorneys general. He stated that the right of a peace officer to enter premises to install or remove an electronic device under the authority of an authorization issued by a judge to intercept telephone communications is possible only if any "terms, conditions, and limitations, included in the authorization are strictly observed". Therefore, in the absence of any limitation on entry into private premises the police officer would be entitled "to enter in order to install (or remove) the device by virtue of section 25 of the Criminal Code and/or section 26(2) of the Interpretation Act, and provided such an entry appears necessary to properly implement the terms of the authorization". As to the right of a police officer to remove an object without the owner's consent in order to install the electronic surveillance device, Mr. Landry had some serious reservations and declined to commit himself one way or the other until the question was examined in depth.

49. By February 13, 1979, after receiving opinions from a number of provincial attorneys general, Mr. Landry's views were strengthened. In a memo of that date, Mr. Landry stated that most of the provinces agreed with his conclusion concerning the first issue stated in his letter of June 9, 1978, though

one province (unspecified) did advance the view that the authorization should contain a clause expressly providing for the installation or removal of the device in order that the peace officer executing the authorization would be protected from civil and criminal liability. With respect to the second issue raised in Mr. Landry's letter there was no consensus among the provinces. Some thought that, in the absence of express removal powers in the authorization, if, for example, a police officer removed a vehicle in order to install a listening device, he would be committing the offence of theft under section 283 of the Criminal Code or the offence of taking a motor vehicle without consent under section 295. Two provinces felt that regardless of the absence of express removal powers in the authorization, a peace officer could take whatever steps were reasonably required to execute the authorization, including the temporary removal of a vehicle. After considering all the opinions Mr. Landry himself opted for the approach that, if it was not specifically provided for by the document authorizing the installation of the electronic surveillance device, then no removal of an object should be undertaken.

50. In December 1977, in *R.* v. *Dass*,[15] Mr. Justice Hamilton of the Manitoba Court of Queen's Bench considered the admissibility of evidence of communications intercepted by use of a listening device installed in premises. He held that an authorization to intercept under section 178.13(2) of the Criminal Code, which extended to both telephonic and oral communications and contained the words "install, make use of, monitor and remove" any device required, authorized a trespass necessary to effect the installation of the device. In April 1979, Mr. Justice Huband in the Manitoba Court of Appeal, delivering the judgment of that court in the *Dass* case,[16] held that evidence obtained from a listening device installed after a surreptitious entry but pursuant to an authorizing order issued under section 178.13 was admissible as "lawfully made" under section 178.16 even if it was made after a break-in, trespass or illegal entry into the premises. He observed:

> How that authorization is carried out is not germane to the issue of the admissibility of evidence flowing from the interception. If a trespass has been committed, then those who have committed the trespass will be answerable in some other criminal or civil forum.

However, in remarks not necessary for the decision but evidently carefully considered, he also specifically rejected an argument presented by Crown Counsel that the authority to install carried with it by implication the authority to enter the premises by force, if necessary, to install the device. Mr. Justice Huband said:[17]

> The order granted by Deniset J. and subsequently renewed by others authorizes the interception, and "for such purposes to install, make use of, monitor and remove" the devices. Crown counsel argues that the authority to install carries with it by implication the authority to enter premises by force or by stealth in order to implant the device.

---

[15] [1978] 3 W.W.R. 762, 3 C.R. (3d) 193, 39 C.C.C. (2d) 465.
[16] [1979] 4 W.W.R. 97.
[17] *Ibid.*, at pp. 116-117.

> As previously noted, the reference to the installation of the authorization order is not a fiat by the courts to violate the laws of the land. I see nothing in the Criminal Code which gives a judge the power to authorize or condone illegal entry. Crown counsel points to s.178.23(2)(d), which appears to enable the judge to impose terms and conditions which he considers advisable in the public interest. In my view, that provision was not intended as a mechanism to have the courts authorize illegal acts. The public interest is not served by acts which violate the civil or criminal laws of the land. The terms and conditions could not validly include permission, directly or by implication, to ignore or breach such laws.

51. Coincidentally, in the same month, the Supreme Court of the United States held in *Dalia* v. *United States*[18] that Congress, in legislating for electronic surveillance under a court order authorizing the installation, maintenance and removal of an interception device, without any statutory limitation on the means necessary to accomplish the electronic surveillance, must have intended to authorize the courts to approve means necessary and reasonable in the circumstances.

52. The R.C.M.P. advised us that as a result of the doubt created by the *Dass* case, some attorneys general issued instructions to the police to cease interceptions where entry was required until the doubt could be removed either by another court or by amendment to the law permitting entry. We requested all attorneys general to inform us as to their position in this regard. A review of the replies received by us indicates that what the R.C.M.P. had told us was correct. Those attorneys general who did not believe that the *Dass* case created doubt as to the legality of entry in appropriate cases cited section 25 of the Code, section 26(2) of the Interpretation Act, and the wording of authorizing orders. One indicated a preference for the reasoning in *Dalia*. Several attorneys general pointed out that, in August 1979, a resolution of the Criminal Law Section of the Uniform Law Conference (a national body formed by the federal and provincial governments to study and encourage uniformity of legislation across Canada) had stated that the power of entry was implied in law. However, the Conference had suggested that the law be amended to provide expressly that an authorization to intercept a private communication under Part IV.1 of the Code be deemed to include authorization to enter premises and install, repair, maintain and remove listening devices, subject to any restrictions imposed by the Court under section 178.13(2)(d).

53. If Mr. Landry's opinion is correct, there are unanswered questions. If a policeman acting under a judicial authorization is on premises surreptitiously to install a listening device, and he is discovered in the act by the occupant who has returned unexpectedly, does the policeman have the implied power, by virtue of section 26(2) of the Interpretation Act, to strike the occupant in order to make his escape? If so, what degree of force may he use? May one of the policemen outside, who is keeping watch, stop the occupant before the occupant reaches his residence, and if "necessary" restrain him by force? Assistant Commissioner Venner told us that the implication is that whatever power is

[18] (1979) 441 U.S. 238.

necessary "within reasonable limits" may be used by the police, who must exercise "judgment" and use "reasonable conduct". He would not assert that such steps would be "legal" but he thought that a policeman would have a defence to a charge (Vol. 33, pp. 5462-7). (We do not know what he meant by drawing the distinction.) We note also that the combined operation of section 26(2) of the Interpretation Act and section 25 of the Criminal Code would, in Mr. Venner's opinion, give the police the power to remove an automobile from its owner's possession in order that a listening device may be secreted in it; at least, there would be "a defence against the charge of theft" (Vol. 33, p. 5463).

54. The same issue applies equally to entry for the purpose of surveying, installing, maintaining and repairing and removing when, pursuant to section 16(2) of the Official Secrets Act, a listening device is to be installed in premises under a warrant of the Solicitor General. Because the procedure employed in conducting electronic eavesdropping under section 16 was, until our public hearings, even less known to the public than that under section 178 of the Criminal Code, and, within the R.C.M.P. and government there does not appear to have been any discussion of this issue in terms of warrants under section 16, there has been little or no analysis of the issue in terms of section 16. However, we do not see any difference between the issue as it arises under section 16 and the issue as it arises under section 178.

55. It will be recalled that *obiter dicta* in the Manitoba Court of Appeal in the *Dass* case said that section 178.13 of the Criminal Code does not empower a judge to include in his authorization a term that authorizes entry into premises for the purpose of installing a listening device. The judgment did not refer to section 25(1) of the Criminal Code or section 26(2) of the Interpretation Act. We understand that those sections were not cited in argument because counsel for the prosecution did not consider them to be relevant. However, that was not the view of the senior officials of the federal Department of Justice in 1979. For example, the Associate Deputy Minister of Justice wrote a letter to the Department of the Solicitor General late in 1979, in respect to a Solicitor General's warrant issued under section 16 of the Official Secrets Act. The opinion expressed in the letter relied not so much on section 26(2) of the Interpretation Act as upon the argument that the legislation could, in large measure, be rendered ineffectual if the interceptions of communications were restricted to those that could be made without any resort to surreptitious or covert entry of premises. Consequently, according to that opinion, only express words or absolutely necessary implication could lead to the construction being properly placed on the legislation that there is no implied power of entry.

56. It therefore becomes necessary to consider those statutory provisions. It will become apparent that in our considered opinion there is real doubt that they support the opinions expressed by the Department of Justice. We say so with considerable boldness and some hesitation, an ambivalence caused by the fact that the opinion of the Department of Justice is supported by the views of some provincial attorneys general and of the Criminal Law Section of the Uniform Law Conference. That being so, we shall give our reasons in some detail.

Does section 25(1) of the Criminal Code justify such an implied power of entry?

57. Section 25(1) derives from a large group of sections in the English Draft Code of 1879, concerning which the Commissioners who had been appointed to consider codifying the criminal law stated that these sections

> . . . contain a series of provisions as to the circumstances which justify the application of force to the person of another against his will. . . We believe that in the main these provisions embody the common law, though on some points they lay down a definite rule where the law is at present doubtful, and in others correct what appear to be defects in the existing law.[19]

The original limitation of the above series of sections, defining the circumstances that justify the *application of force to the person of another*, is still evident throughout sections 25 to 33 of the present Code, wherein constant reference is made to "using as much force as is necessary" or "uses no more force than is reasonably necessary". The same theme is evident in section 25(3) which defines the circumstances in which the use of force that is intended to cause death or grievous bodily harm is justifiable, and in section 25(4) in which the acceptable limits to the use of violence against a person who takes flight to avoid arrest are set forth. It is, therefore, not in our view permissible to suggest that section 25(1) contains a blanket dispensation to peace officers to act in a manner proscribed under the Criminal Code or the common law (e.g. of trespass) in the course of effecting an arrest, or executing a court order or judicial authorization. Moreover, the opinions of the Department of Justice made no reference to the view expressed in the Supreme Court of Canada in *Eccles* v. *Bourque*.[20] The significant issue in that case, for our present purposes, was whether a peace officer who is authorized under section 450(1)(a) of the Code to make an arrest without warrant is also authorized by section 25 to commit a trespass, with or without force, in the accomplishment of that arrest. Five members of the Court were content to reserve their answer to this question until a later occasion. Mr. Justice Dickson, however, in an opinion that was concurred in by three other judges, said:[21]

> It is the submission of counsel for the respondents that a person who is by s.450 authorized to make an arrest is, by s.25, authorized by law to commit a trespass with or without force in the accomplishment of that arrest, provided he acts on reasonable and probable grounds. I cannot agree with this submission. Section 25 does not have such amplitude. The section merely affords justification to a person for doing what he is required or authorized by law to do in the administration or enforcement of the law, if he acts on reasonable and probable grounds, and for using necessary force for the purpose. The question which must be answered in this case, then, is whether the respondents were required or authorized by law to commit a trespass; and not, as their counsel contends, whether they were required or authorized to make an arrest. If they were authorized by law to commit a trespass, the authority for it must be found in the common law for there is nothing in the Criminal Code.

[19] Cmnd. 2345, p. 18.

[20] (1974) 19 C.C.C. (2d) 129.

[21] At p. 130-31.

The same line of reasoning was apparent in the judgment of Mr. Justice Robertson in the earlier disposition of the same case by the British Columbia Court of Appeal:[22]

> . . . it cannot fairly be said that a person who is authorized to make an arrest is, because of s.25, authorized by law to commit a trespass with or without the use of force. In other words, wherever the Criminal Code confers a power to do a specific thing, s.25 does not confer a power to do any and every thing that may assist or advance the exercise of the power. The purpose of s.25(1) is twofold; it absolves of blame anyone who does something that he is required or authorized by law to do, and it empowers such person to use as much force as is necessary for the purpose of doing it.

Another member of the court, Mr. Justice Nemetz did not express any opinion on the scope of section 25(1) other than to observe:

> . . . it is clear to me that, although police officers may arrest without warrant (s.450), scrupulous adherence must be had for the principles set out at common law respecting the procedures that are to be used by police in entering a house without warrant. I do not read s.25(1) as giving a police officer the right forcibly to enter a stranger's home when he is seeking the arrest of a fugitive unless he can justify such forcible entrance on reasonable and probable grounds.

In our view, the opinions of the Department of Justice have failed to take into account the limits of the extent to which section 25(1) affords the power to commit what would ordinarily be trespass or theft. In our opinion, if Mr. Justice Dickson's judgment in *Eccles* v. *Bourque* is (as we think) correct, it requires one to look not to section 25(1) but to the common law for justification for the police power that is asserted. In that case, he found that the common law did empower entry upon premises in order to effect an arrest. In the case of the investigative technique which we are examining, there is no common law precedent of which we are aware which may be called in aid of the power of a peace officer to commit theft or trespass when authorized to install a listening device.

Does section 26(2) of the Interpretation Act justify an implied power of entry?

58. Section 26(2) of the Interpretation Act has already been quoted. Does it apply to an authorization by a judge given under section 178.13 of the Criminal Code or to a warrant issued by the Solicitor General under section 16(2) of the Official Secrets Act? The Act applies to 'enactments', not to judicial orders made pursuant to an enactment. Thus, it could be argued that the power to trespass in order to install a device is implied in section 178; if that is so, there would be an implied statutory power that would permit a judge to include the power of entry in the authorization. However, in the absence of any such term in the authorization, the issue would still remain: is there an implied power of entry once an authorization is granted?

59. In our view, it is doubtful that these provisions provide a defence in law for what otherwise would be theft or trespass. Those who argue that the

[22] (1974) 14 C.C.C. (2d) 279.

Manitoba Court of Appeal in *Dass* was wrong point to the decision of the Supreme Court of the United States in *Dalia* v. *United States*. There, the majority opinion was that the power of surreptitious entry was necessarily implied in the statute that authorized the courts to review and approve electronic surveillance applications. However, in assessing the reasoning of the majority opinion in *Dalia* v. *United States* it is important to note that it emphasized the legislative history of the statute; there was evidence from the Congressional Record that Congress was aware that "most bugging requires covert entry". The opinion also stressed the importance of the fact that "Absent covert entry... almost all electronic bugging would be impossible". In Canada, it is far from clear that either of these points was known to Parliament when the Protection of Privacy Act was passed. Moreover, frequently the entry needed may not be "covert" at all from the point of view of the person who is the owner or occupier at the time of entry — as, for example, a hotel manager who gives permission for the entry before the hotel room is occupied by the suspect, or even while it is occupied by a short-term guest. In such cases there would be no trespass. Many buggings arise in just such situations. Therefore it is not clear to us that Parliament must have realized it was implicitly authorizing trespassory covert entries.

60. However, there is a recent judgment of the British Columbia Court of Appeal in another case, which upheld the implied power of a peace officer to enter a residence to execute a warrant issued under the section of the Code that permits the seizure of firearms.[23] The court held, quite briefly, that in order to give effect to the intent of the section, "we should hold" that the authority to seize "includes the right to search... and includes the right to enter on a person's property to make the search". This decision is a sufficient reminder that a court other than the Manitoba Court of Appeal might reach a conclusion that trespassory entry for the purpose of installation is necessary in order to give effect to a "paramount" public interest to which "the rights of the individual are secondary".[24] Yet, in our view, it is not easy to reconcile the approach of the British Columbia Court of Appeal with that of Mr. Justice Dickson in *Eccles* v. *Bourque*.*

61. In Part X, Chapter 1 we discuss the recent decision of the highest court of England, the House of Lords, in *Morris* v. *Beardmore*. There it was held that a statute that empowered a uniformed police officer to require a person to give a breath sample could not by implication permit an officer to trespass in the suspect's home in order to make the demand. Consequently, if a demand were made during the course of such trespass, the demand would be unlawful and there could not be a conviction for refusal to comply. Lord Diplock said that, "if Parliament intends to authorize the doing of an act which would constitute a tort actionable at the suit of the person to whom the act is done", there must be an express provision to that effect in the statute. He stated that

---

[23] *R.* v. *Colet* [1979] 2 W.W.R. 267.

[24] Using the language of Craig, J.A. who delivered the judgment of the British Columbia Court of Appeal, in respect of the section he was interpreting.

> The presumption is that in the absence of express provision to the contrary Parliament did not intend to authorize tortious conduct.[25]

Applying that reasoning to the *Dass* situation, we believe that it cannot be inferred that Parliament, in enacting a general provision such as is found in section 26(2) of the Interpretation Act, intended that otherwise unlawful powers are deemed to be given to the officer to enable him to do the act which he is empowered to do.

62. We have already mentioned that in August 1979, the Criminal Law Section of the Uniform Law Conference adopted a resolution. Its full terms are as follows:

> WHEREAS the Commissioners are of the view that section 25 of the Criminal Code and section 26 of the Interpretation Act constitute sufficient authority to make it clear for the purposes of Part IV.1 of the Code that lawful authority to intercept includes authority to enter premises and install, repair, maintain and remove listening devices; and
>
> WHEREAS the Commissioners also recognize that the *Dass* case has created sufficient doubt in this area to place the police in a position of uncertainty;
> Be it resolved
>
> that Part IV.1 of the Criminal Code be amended to provide that an authorization to intercept a private communication is deemed to include authorization to enter premises and install, repair, maintain and remove listening devices, subject to any restriction imposed by the Court under s.178.13(2)(d).

[25] [1980] 3 Weekly L.R. 283 at 289.

* On January 27, 1981, four days after this Report was delivered to the Governor in Council, the Supreme Court of Canada delivered judgment in the *Colet* case. In a unanimous judgment delivered by Mr. Justice Ritchie, the judgment of the British Columbia Court of Appeal was reversed and the reasoning of the trial judge was adopted. The trial judge had pointed out that when, in the Criminal Code, Parliament sought to include the right to search in providing for the authority to seize, it did so in specific terms. The court quoted with approval from the judgment of Mr. Justice Dickson in *Eccles* v. *Bourque* and repeated the "common law principle" which "has been firmly engrafted in our law since *Semayne's* case", that "the house of every one is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose...". Mr. Justice Ritchie rejected the argument of the Court of Appeal and said:

> . . . it would in my view be dangerous indeed to hold that the private rights of the individual to the exclusive enjoyment of his own property are to be subject to invasion by police officers whenever they can be said to be acting in the furtherance of the enforcement of any section of the Criminal Code although they are not armed with express authority to justify their action.

Finally, Mr. Justice Ritchie held that section 26(2) of the Interpretation Act could ". . . not be considered as clothing police officers by implication with authority to search when s.105(1) and the warrant issued pursuant thereto are limited to seizure".

The Commissioners did not comment on whether they considered that a present "lawful authority to intercept" includes authority to remove a vehicle from the owner's control, or to use the target's power supply to operate the device, or to use force to restrain a person who appears on the scene.

63. The recommendation of the Uniform Law Commissioners would satisfy the following observation by the Ontario Royal Commission of Inquiry into Civil Rights, chaired by Chief Justice J.C. McRuer:[26]

> When legislation is drawn which is intended to give the power of entry to premises, the power should be stated in clear terms so that when it comes before the members of the Legislature they will know what they are voting on. They ought not to be left to examine the Interpretation Act, or the law applicable to implied powers, when they are required to vote for or against legislation purporting to authorize rights of entry to private property.

If the amendment recommended by the Uniform Law Commissioners is adopted by Parliament, the amendment should be as clear as possible as to whether the police or the security intelligence agency, in exercising the authority granted by the means provided by statute, have all the specific powers that may be required in order successfully to conduct an electronic surveillance operation from beginning to end. The kinds of powers that legislative attention must be addressed to are found in our recommendations in Part V, Chapter 4 and Part X, Chapter 5. If the word "premises" is to include a vehicle or other things, the amendment should be clear whether there is to be a power to remove a thing temporarily without the consent of the person entitled to possession.

64. The power to enter must be strictly circumscribed to prevent any possibility of persons acting under the warrant, in the event of being surprised in the procedure of installation, maintenance, repair or removal, using any physical force against any other person. In the absence of strict statutory prohibition of the use of such force, there is a serious risk that the policeman acting under the authority of a judicial authorization or members of the security intelligence agency acting under a Solicitor General's warrant might consider themselves authorized to use force to restrain a person surprising them during the course of the operation. The danger of this occurring is supported by the opinion given by the Deputy Minister of Justice on February 10, 1978, which stated:

> Subsection 25(1) of the Criminal Code provides, in part, that everyone who is required or authorized by law to do anything in the administration or enforcement of the law as a peace officer is, if he acts on reasonable and probable grounds, justified in doing what he is required or authorized to do and in using as much force as is necessary for that purpose. By virtue of subsection 25(3) a person is not justified in using force that is intended or is likely to cause death or grievous bodily harm, unless he believes on reasonable and probable grounds that it is necessary for the purpose of preserving himself or anything under his protection from death or grievous bodily harm.

---

[26] *Report of the Ontario Royal Commission of Inquiry into Civil Rights*, Toronto, 1968, Vol. 1 at p. 411.

65. For the sake of discussion, let us assume that the intention of Parliament was to enable police officers, armed with a judge's authorization under section 178 of the Criminal Code or a Solicitor General's warrant under section 16 of the Official Secrets Act, to enter premises, remove vehicles, use the target's electrical power supply or restrain persons interfering. If sections 25(1) of the Criminal Code and 26(2) of the Interpretation Act do not entitle a judge or Solicitor General to include express terms to that effect in the authorization or warrant, and if those statutory provisions do not imply such powers where the authorization or warrant is silent, then Parliament's intention is frustrated. However, this would not be the first time that the intention of Parliament has been frustrated by the failure to use language sufficiently clear to give effect to its intention. The remedy is to enact more explicit statutory provisions. It is unsatisfactory to leave these issues unresolved, for otherwise the police and the security intelligence agency will be left uncertain as to the extent to which they are protected by such provisions as section 26(2) of the Interpretation Act and section 25 of the Criminal Code.

66. In Canada the existence of an implied power to enter and do the other things necessary for a successful electronic surveillance, once an authorization or warrant is issued, is uncertain, and so is the power of a judge or the Solicitor General to insert a term in the authorization permitting such entry. 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". He continued:

> Briefly, these amendments would require (1) that the application for an order authorizing the interception of communications state whether surreptitious entry will be required to effect the interception and, if so, why other means of effecting the interception are not believed to be feasible, (2) that the issuing judge make a finding that such entry appears necessary under the circumstances, and (3) that the order approving the interception specifically state whether surreptitious entry for the purpose of effecting the interception is authorized.[27]

Therefore we shall recommend in Part V, Chapter 4 that the statutory provision replacing section 16 of the Official Secrets Act specify the incidental powers that are available to those acting pursuant to a warrant; and in Part X, Chapter 5 we shall recommend that section 178 of the Criminal Code be amended by specifying the incidental powers that are available to those acting pursuant to a judicial authorization.

"Rummaging"

67. Another issue common to both the Security Service and the C.I.B. is whether policemen inside premises to install a listening device, having obtained

[27] Statement of Philip B. Heyman before the Committee on the Judiciary, Subcommittee on Criminal Justice, United States Senate, concerning s.1717, March 5, 1980.

either a judicial authorization under section 178 of the Criminal Code or a Solicitor General's warrant under section 16 of the Official Secrets Act, are at liberty to look around, to search for things or documents of possible interest, and to examine and read and photograph what they find of interest? In other words, may they lawfully conduct an intelligence probe? If they may, must it be limited to observing and photographing what is visible to the naked eye without "rummaging", or is the power unlimited? As has been seen in Chapter 2 of this Part, there are judicial decisions which allow the police latitude, when executing a search warrant, lawfully to seize things found by them on the premises even though those things are not referred to in the search warrant. Does the same latitude apply to authorizations and warrants that are *not* warrants to search and seize? In principle there is no practical way of preventing policemen from observing what is readily visible on the premises where the installation is being made, and merely seeing (even with a photographic eye) is no trespass. However, the moment the policeman begins to look through documents, even though their top page is visible, or to open drawers or luggage, there is conduct that is far beyond the necessary activity associated with the installation of a listening device and there may be a trespass. As far as judicial decisions are concerned, there does not appear to be any authority on the point. In Chapter 2 of this part of our Report we saw that there are cases which have held that, within certain limits, a policeman does not become liable for damages for trespass if he exceeds his authority under the search warrant. *Chic Fashions (West Wales), Ltd.* v. *Jones*,[28] which was concerned with search warrants for stolen goods, held that a peace officer may seize under warrant goods not specified in the warrant when he reasonably believes them to have been stolen and to be material evidence on a charge of stealing or receiving against the person in possession of them or anyone associated with him. *Ghani* v. *Jones*[29] suggests that a peace officer may seize from premises which he has entered under warrant, any material of evidential value in connection with the crime he is investigating, whether against the person he is investigating or anyone associated with him in the offence. These English decisions, if they are applied by Canadian courts, go far in permitting policemen to search and seize beyond the terms of a search warrant. Yet they, and earlier authority to the same effect,[30] do not appear to us to support the power of peace officers, armed with an 'authorization' or a 'warrant' to *intercept communications*, to conduct a *search for things*. While the cases cited may be correct in allowing search and seizure of things *beyond the authority of a warrant*, we find it difficult to accept as valid the analogy between that situation and a search when an authorization or warrant does not authorize *any* 'search'. Consequently we entertain, at the very least, serious doubt that there is in law any power to search and look at things while on premises pursuant to an authorization given under section 178.13 of the Criminal Code or a warrant issued under section 16(2) of the Official Secrets Act. Any such power should be provided for in the warrant for surreptitious entry which, as we have indicated in Chapter 2 of this Part, should be granted only in security cases.

[28] [1968] 2 Q.B. 299; [1968] 1 All E.R. 229.
[29] [1970] 1 Q.B. 693; [1969] 3 All E.R. 720.
[30] e.g. *Elias* v. *Pasmore* [1934] 2 K.B. 164.

(b) *Legal and policy issues unique to Security Service*

68. We turn now to a consideration of the procedures adopted when warrants have been applied for under section 16(2) of the Official Secrets Act, which came into effect on July 1, 1974. It will be recalled that this section was passed as part of the Protection of Privacy Act. That statute made it an offence (under Part IV.1 of the Criminal Code and particularly section 178.11(1)) to intercept a private communication wilfully by means of an electromagnetic, acoustic, mechanical or other device, unless the person intercepting has the consent of one of the parties or a judicial authorization. (There are additional protections — for example, for telephone company employees engaged in checking the equipment.) A further defence is provided by section 16(1) for a person who makes an interception pursuant to a warrant issued by the Solicitor General under section 16(2). At this point it is desirable to set forth all the amendments to the Official Secrets Act contained in the Protection of Privacy Act:

> 5. Subsection 2(1) of the Official Secrets Act is amended by adding thereto, immediately after the definition "document", the following definition:
>
> "intercept" includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof.
>
> 6. The said Act is further amended by adding thereto the following section:
>
> 16. (1) Part IV.1 of the Criminal Code does not apply to any person who makes an interception pursuant to a warrant or to any person who in good faith aids in any way a person whom he has reasonable and probable grounds to believe is acting in accordance with a warrant, and does not affect the admissibility of any evidence obtained thereby and no action lies under Part I.1 of the Crown Liability Act in respect of such an interception.
>
> (2) The Solicitor General of Canada may issue a warrant authorizing the interception or seizure of any communication if he is satisfied by evidence on oath that such interception or seizure is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.
>
> (3) For the purposes of subsection (2), "subversive activity" means
>
> (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.
>
> (4) A warrant issued pursuant to subsection (2) shall specify
>
> (a) the type of communication to be intercepted or seized;
>
> (b) the person or persons who may make the interception or seizure; and
>
> (c) the length of time for which the warrant is in force.

(5) The Solicitor General of Canada shall, as soon as possible after the end of each year, prepare a report relating to warrants issued pursuant to subsection (2) and to interceptions and seizures made thereunder in the immediately preceding year setting forth

(a) the number of warrants issued pursuant to subsection (2),

(b) the average length of time for which warrants were in force,

(c) a general description of the methods of interception or seizure utilized under the warrants, and

(d) a general assessment of the importance of warrants issued pursuant to subsection (2) for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada and for the purpose of gathering foreign intelligence information essential to the security of Canada, and a copy of each such report shall be laid before Parliament forthwith upon completion thereof or, if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting.

Warrants issued before July 1, 1974

69. Before section 16 of the Official Secrets Act came into effect on July 1, 1974, the Security Service wanted to ensure the continuance, without interruption, of telecommunications intercepts and electronic listening devices already installed and in use. Consequently, from June 14, 1974 until the end of that month, the Director General applied for, and the Solicitor General, Mr. Allmand, signed approximately 242 warrants, purporting to be pursuant to section 16 of the Official Secrets Act (Vol. 162, p. 24855). The number 242, which was given *in camera* (Vol. C71, p. 9951), was inadvertently not published in the publicly released version of that evidence. No one — whether Mr. Allmand or Mr. Dare or anyone else — appears to have addressed the question as to whether such warrants had any legal effect on and after July 1. In our view they did not. A statute cannot speak except from the time it comes into effect, and section 16 of the Official Secrets Act did not come into effect until July 1. Only on and after that date could a warrant be issued which would have any status in law. If Parliament intended to give effect to a warrant signed on a date earlier than the date on which the statute came into effect, it would have said so. As a result, in our opinion, although everyone concerned acted in good faith, these warrants were invalid, and in theory those who acted upon them after June 30, 1974 might be open to a charge under section 178 of the Code. We do not think that in the circumstances anyone would think that such charges should be laid. A broader lesson for the future that is afforded by this issue is the need for the security intelligence agency and the Solicitor General having at their disposal informed and competent legal advice, so that issues of this kind may more likely be identified instead of being passed over, unnoticed and unconsidered.

Legal and policy issues relating to the procedure of applying for warrants

70. The following are points arising from the present practice of making applications to the Solicitor General under section 16. A number of the points

give rise to legal concerns, some of which may have escaped the perception of the Director General and his subordinates, and the Solicitor General.

(i) *Renewal procedure*

71. In December of each of the years from 1974 to 1978 the Director General presented to the Solicitor General a document entitled "Application for the Renewal of Warrants to Intercept and/or Seize", which reads as follows:

> This is the application of Michael R. Dare, a member of the Royal Canadian Mounted Police, hereinafter called the applicant, taken before me.
>
> The applicant says he has personally reviewed the applications to obtain warrants to intercept and/or seize, sworn by him during the year 1974, hereinafter called the applications.
>
> The applicant further says in the applications numbered [there followed the number of applications made during the year] his reasonable grounds for suspecting that the communications described therein, or some part of them, are passing, or will pass, still exist.
>
> NOW THEREFORE the applicant prays that the warrants to intercept and/or seize corresponding to the said applications and which would otherwise expire on December 31, 1974, may be renewed.

The Solicitor General then signed a document entitled "Renewal of Warrants to Intercept and/or seize", reading as follows:

> To: The Director General, Security Service, Royal Canadian Mounted Police, and the members and agents of the Royal Canadian Mounted Police acting under his authority or on his behalf.
>
> WHEREAS the Warrants to Intercept and/or Seize under the Official Secrets Act signed by me during the year 1974 are due to expire on December 31, 1974.
>
> AND WHEREAS I am satisfied by evidence on oath of Michael R. DARE, a member of the Royal Canadian Mounted Police, that he has personally reviewed the Applications to obtain the said Warrants sworn by him during the year 1974, and that in the Applications numbered [here the numbers of warrants are inserted] his reasonable grounds for suspecting that the communications described therein, or some part of them, are passing, or will pass, still exist.
>
> NOW THEREFORE you are hereby authorized during the period from the 1st day of January, 1975, to the 31st day of December, 1975, to continue to intercept and/or seize communications under the Warrants signed by me corresponding to the Applications above listed.

As we pointed out earlier there is no provision in section 16 of the Official Secrets Act for renewals of warrants. By way of contrast, section 178.13(3) of the Criminal Code expressly provides that a judge may grant "renewals of an authorization" from time to time. Both sections were enacted in the Protection of Privacy Act. It is a general principle of statutory construction that the statute must be read as a whole, so that if in one circumstance the statute provides for the doing of a thing but in another circumstance the statute does

not provide for the doing of that thing, in the second circumstance it may be inferred that the statute does not authorize the doing of the thing. Applying that principle, in our view there is no statutory authority for the granting of "renewals" of warrants. The result is that a large number of warrants between June and December 1974, all of which were framed so as to expire on December 31, 1974, were not in law effective beyond December 31, 1974. A number of the 1974 warrants were the subject of so-called renewals at the end of 1975, 1976, 1977 and 1978, and were considered by the Security Service to be valid and operative until December 31, 1979. Some of them, of course, were cancelled or allowed to lapse at the end of a calendar year during that period. More warrants were issued in 1975 and were the subject of purported renewal at the end of 1975 and in the succeeding years; and the same was true of new warrants issued in 1976, 1977 and 1978. Thus, during the entire period from January 1, 1975 until December 31, 1978, if we are right in our view of the law, the Solicitor General, lacking the advice of either his Deputy Minister or of the Department of Justice, by signing the so-called "renewal of warrants" each December until 1978, may have inadvertently exposed the members of the R.C.M.P. acting upon the documents to the theoretical possibility of prosecution. However, no doubt, in considering whether those members should be charged under section 178, the Attorney General of Canada or of a province would take into account that the members were relying upon purported renewals of the warrants signed by the Solicitor General of Canada. Moreover, the Attorney General should take into account that on the first occasion when this procedure was used, in December 1974, the renewal forms had been approved by a senior member of the Department of Justice, although it does not appear that any written legal opinion was given by that member of the Department of Justice as to the validity of the procedure which preparation and approval of the forms clearly contemplated would take place each December. In Part V, Chapter 4, we shall make a recommendation as to the procedure which should be provided for by statute when warrants expire.

72. Lest anyone should think that our approach is unduly technical, we hasten to add that there are sound policy grounds for criticizing the procedure adopted in the years 1974 to 1978, in obtaining "renewals". The policy of the statute, as expressed in section 16(2), requires the Solicitor General to be satisfied by evidence on oath "that such interception or seizure is *necessary*" (our emphasis) for one of three purposes. This is a statutory criterion which cannot be satisfied unless there is information placed before the Solicitor General on oath as to why he should find necessity to exist in the circumstances. The so-called applications sworn to by the Director General before the Solicitor General in December of each of the years from 1974 to 1978 did not set forth any grounds upon which the Solicitor General might find that necessity existed. All that the Director General stated on oath was that he had "reasonable grounds for suspecting that the communications described therein, or some part of them, are passing, or will pass, still exist". Thus, even if the applications for "renewal" are looked upon as if they had been styled "applications", and if the "renewal" were treated as if it were a series of "warrants", there was no "evidence" of necessity given on oath, on the basis of which the Solicitor General could grant such "warrants".

(ii) *Swearing of evidence under oath*

73. Section 16(2) authorizes the Solicitor General to issue a warrant "if he is satisfied by evidence on oath". During the early years of the use of section 16, the so-called "application", which was the document purportedly sworn by Mr. Dare, was frequently very brief in terms of describing the activities of the target person or organization, and it stretches the imagination to claim that the bald statement that "such interception or seizure is necessary..." constituted the requisite "evidence on oath" that such interception or seizure was necessary. However, the practice also developed that *aide-mémoires* would be prepared, and that Mr. Dare would bring these with him and show them to the Solicitor General together with the "application". The *aide-mémoire* was not a schedule or annex to the "application", and thus, on the face of the documentation, there was no indication that the truth of the contents of the *aide-mémoire* was sworn to on oath by Mr. Dare. Indeed, Mr. Dare's own evidence was that he did not consider that he was swearing to the truth of the contents of the *aide-mémoire* (Vol. 126, pp. 19647-8). (The accompanying memorandum was, however, being referred to in the form of oath used by Mr. Dare by April 8, 1980, when he last testified on the subject (vol. C88, p. 12186).) Yet Mr. Allmand has testified that he considered that Mr. Dare, in taking the oath before him, was swearing to the truth of all the information which Mr. Dare presented to him (Vol. 115, p. 17756). The Deputy Solicitor General, Mr. Tassé, who was present on many of these occasions, testified that it was customary that Mr. Dare, with Bible in hand, swore "to tell the truth, the whole truth, and nothing but the truth". Although Mr. Tassé understood that Mr. Dare was swearing to the truth of his affirmations or comments, Mr. Tassé did not testify that in the form of oath there was any specific reference to the "evidence" to be found either in the "application" or in the *aide-mémoire* (Vol. 156, p. 23828). Mr. Dare himself testified as to the procedure he was following:

> If it is one or more than one, I stand and take the Bible in my hand and make my attestation. I identify myself as a member of the Royal Canadian Mounted Police, do solemnly swear this or these warrants are required for the security of Canada under the Official Secrets Act. The applicable section of the Act is sworn on each of the warrants.
>
> (Vol. C88, p. 12186.)

He said that "that was the form of oath", although by the time that he testified on April 8, 1980, the word "warrants" is followed by the words "and the accompanying memorandum" (Vol. C88, p. 12186). Thus, if Mr. Dare's evidence is accepted — and it is he who has been personally involved for six years — then it would appear that this practice, as described, has not resulted at all in his swearing to the truth of the statements of fact contained in the application or in the *aide-mémoire*. What he has apparently done is no more than swear to the warrants being "required". (See, in addition to the above testimony, his earlier testimony at Vol. 126, p. 19649.) If his evidence is accepted, then his practice has failed to satisfy the requirement of the statute, for the "evidence" is not "on oath". We do not question the sincerity of Mr. Dare or his subordinates in preparing the material in support of the applica-

tions for warrants or in attempting to comply with the statute. However, the form prescribed by statute was intended to provide some assurance that a Solicitor General would act only on the basis of "evidence" which some person was prepared to verify "on oath". Bearing in mind that the entire procedure by its very nature is very secret, and will never be examined (apart from a Commission of Inquiry such as ours) by any tribunal or by Parliament, it then becomes more than just a matter of form, but rather a matter of form becoming substance, to do the utmost to ensure that the procedure is treated with all the seriousness that is deserved by intrusions into privacy which are numerous and frequently perennial. In Part V, Chapter 4, we shall recommend that the truth of all of the evidence should be sworn to under oath. Here, however, we might add again that the problem we have identified might have been avoided, had legal advice been obtained as to the proper form of the oath to be sworn on these occasions.

(iii) *Identification of the statutory basis in the warrant itself*

74. The warrants issued by the Solicitors General since June 1974 have suffered from what in our opinion is a serious defect. Section 16(2) provides that the Solicitor General may issue a warrant for wiretapping if he is satisfied by evidence on oath that one of the following facts exists:

— that such interception is necessary for the prevention or detection of subversive activity directed against Canada;

— that such interception is necessary for the prevention or detection of subversive activity . . .detrimental to the security of Canada;

— that such interception is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.

The practice has been that the warrants have simply recited that the Solicitor General is

> satisfied by evidence on oath of Michael R. Dare, a member of the Royal Canadian Mounted Police, that it is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada to intercept and/or seize any communication hereinafter described. . .

When a search warrant is issued under section 443 of the Criminal Code, it has been held that the offence must be referred to in the warrant.[31] One of the reasons for such a requirement is so that the person whose premises are searched and anyone concerned will know what the alleged offence is, about which evidence is being sought. This reason is inapplicable to warrants issued under section 16(2) of the Official Secrets Act, but another reason may be pertinent: that naming the offence in the search warrant is evidence that the

[31] *R.* v. *Read, ex p. Bird Construction Ltd.* [1966] 2 C.C.C. 137 (Alta S.C.); *Re McAvoy* (1971) 12 C.R.N.S. 56 (N.W.T.S.C.); *Royal American Shows Inc.* v. *The Queen, ex. rel. Hahn* [1975] 6 W.W.R.571 (Alta. S.C.); *PSI Mind Development Institute Ltd.* v. *The Queen* (1977) 37 C.C.C. (2d) 263 (Ont. H.C.J.). There is disagreement in these cases only as to the degree of particularity required to be stated.

justice has exercised his discretion judicially in issuing the search warrant. The same may be said of warrants issued by the Solicitor General under section 16(2): identification of the specific activities being investigated, that is in terms of the three possible alternatives referred to in the subsection, would be evidence that the Minister had exercised his statutory powers with the required degree of attention to the law. Perhaps this would be unimportant if the "evidence on oath" directed the Minister's attention to one of the three heads. However, the so-called "applications" which are the "evidence on oath" have usually *not* indicated which category Mr. Dare has considered the circumstances to fall within. In Part V, Chapter 4 we consider this matter further and make recommendations.

Problems in interpreting the meaning of "subversive activity" (section 16(3))

(i) *"Sabotage"*

75. No warrants have yet been issued under section 16(3)(a) of the Official Secrets Act where the allegation is that the activity in question is "sabotage". However, the Security Service has raised with us a question of definition of "sabotage" as used in this section. The issue is whether the word "sabotage" as used in the section is limited to the traditional dictionary definition of sabotage, i.e. "the malicious waste or destruction of property or manufacturing equipment"? Or, on the other hand, could a warrant be issued where the nature of the sabotage was a systematic sabotage of the "effectiveness or credibility of a federal government institution through the systematic leakage of sensitive or classified documentation entrusted to that person's care"? In the opinion of the Security Service, such systematic leakage "designed to discredit or sabotage the effectiveness of a federal government institution, such as the R.C.M.P. Security Service, could be interpreted as an act to retard an essential public service". The Security Service points to Webster's New International Dictionary, Second Edition, as putting forward a second definition of "sabotage",

> Commission by a civilian or enemy agent within a country of any destructive act designed to impede the Armed Forces, or any act or neglect that retards essential industry, public services, etc.

In our opinion, the word "sabotage" in the absence of any indication to the contrary in the statute, should be interpreted in the normal sense in which it is used as a title to section 52 of the Criminal Code, which makes it an offence to do

> a prohibited act for a purpose prejudicial to
>
> (a) the safety, security or defence of Canada, or
>
> (b) the safety or security of the naval, army or air forces of any state other than Canada that are lawfully present in Canada.

Section 52(2) defines "prohibited act" as meaning

> An act or omission that
>
> (a) impairs the efficiency or impedes the working of any vessel, vehicle, aircraft, machinery, apparatus or other thing, or

(b) causes property, by whomsoever it may be owned, to be lost, damaged or destroyed.

(ii) *"Governmental change"*

76. There is a question as to the meaning of the phrase "activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means" as used in section 16(3)(c). Does it include only activities directed towards the overthrow of a government, or does it cover also activities directed toward accomplishing changes of governmental policies and legislation? The latter appears to be the interpretation of the Security Service, and warrants have been obtained under section 16(3)(c) when the evidence presented to the Solicitor General has in no way suggested that the target person or group had as his or its object anything in the nature of revolution. On the other hand, the former Deputy Solicitor General, Mr. Tassé, has testified that it was his opinion that the narrower interpretation was the correct one, based on the equality of the two official languages for purposes of interpreting a statute, and the fact that the French version of the subsection refers to "changement de gouvernement" (Vol. 157, p. 23884). It is by no means clear that those in the Security Service responsible for the preparation of applications have been aware of that opinion or acted upon it. In Part V, Chapter 4 we shall make recommendations to overcome this ambiguity and narrow the meaning of "subversion".

77. A second question arising in the interpretation of section 16(3)(c), about which the Security Service has expressed concern, is whether it applies to activities by a domestic terrorist group whose activities are politically motivated. We see no problem. As "terrorism" is defined as "violence for political ends", the question itself is redundant. In our view, a domestic terrorist group whose objects fall within section 16(3)(c) in all other respects is one whose activities are covered by the subsection.

78. The Security Service is also concerned as to whether section 16(3)(c) applies to activities directed toward governmental change at provincial and municipal levels. In our view such activities are covered by the section. Some members of the Security Service raise the issue whether the words found in section 16(2) "subversive activity... detrimental to the security of Canada" cover activities that would adversely affect Canadian economic security. The matter has never been put to the test by way of an application to a Solicitor General for a warrant, or even by way of preparing such an application nor does it appear that a legal opinion has ever been sought from the Department of Justice. However, our view is that the intent of section 16(2) is that a warrant may be issued under section 16(2) in respect to "subversive activity" only where there is a form of activity falling within the definition of subversive activity found in section 16(3). Only section 16(3)(b) could apply to the economic field. In our opinion, if the suspected activities were foreign intelligence activities directed toward gathering economic intelligence information relating to Canada, that might not be "detrimental to the security of Canada" in the physical sense, but it would be activity "directed against Canada". Therefore the Solicitor General would be authorized to issue a warrant if he

were satisfied by evidence on oath of the necessity of the interception or seizure of a communication involved in such activity.

(iii) *"Governmental change outside Canada"*

79. An issue of serious concern to the Security Service since January 1978 has been whether section 16(2) authorizes the issue of a warrant where the activity within Canada is directed toward violent governmental change outside Canada. Until January 1978 the Security Service had been under the impression that it could obtain warrants, and it did in fact obtain warrants, where the activities of a person or persons within Canada had been directed toward accomplishing governmental change elsewhere than in Canada by force or violence. Thus, the Security Service had obtained warrants where it could satisfy the Solicitor General that interception or seizure of communications was necessary for the prevention or detection of activity of persons connected with various foreign terrorist organizations. However, in January 1978 the newly arrived Department of Justice counsel gave his opinion that warrants could not be issued in such cases because the governing subsection is subsection (2), which requires that the Solicitor General be satisfied that the interception or seizure of a communication is necessary for one of the following situations:

— the prevention or detection of subversive activity directed against Canada,

— the prevention or detection of subversive activity detrimental to the security of Canada, or

— for the purpose of gathering foreign intelligence information essential to the security of Canada.

Thus, although the activity concerned might fall within the definition found in section 16(3)(c) ("activities directed toward accomplishing governmental change... elsewhere...") it did not fall within any of the above three categories, for, in the opinion of the Department of Justice counsel, such activity was not "directed against Canada" or "detrimental to the security of Canada", or (more obviously) "gathering intelligence information essential to the security of Canada". As a result of his opinion, warrants have not been sought since that time, where the planning takes place in Canada but the target is another country. Examples are the following:

— A landed immigrant was thought to be the leader of a "Liberation Movement" of a foreign country. The field unit represented that there was no way to penetrate the group by human sources, and that therefore electronic eavesdropping was the only way of determining to what degree the organization was involved with a Canadian group considered to be "subversive" or what it was doing that might be detrimental to the security of Canada.

— An application was not processed where the targetted individual was said to be an organizer of a dissident movement in a foreign country where that movement was banned. The Security Service field unit described the movement as pro-Soviet and as advocating the overthrow of its own government.

— A similar example was that of a proposed warrant against communications of a foreign "leftist" thought to belong to a revolutionary movement in his country of origin and to be a leader of his countrymen in a Canadian city.

80. We question the correctness of the legal opinion upon which this reticence by the Security Service has been founded since 1978. We recognize that the matter is not free from doubt, and we certainly do not criticize counsel for the Department of Justice for giving the opinion which he gave. Our view is based on mounting experience around the world, that one of the increasingly common ways in which terrorist groups attack a country is not within its own borders but outside its borders, as for example, by attacks on that country's missions abroad or its mission personnel abroad. Thus, there is a strong possibility that a foreign terrorist group whose members in Canada are suspected of actively planning terrorist acts against their homeland may plan to do so by attacking the mission premises or mission personnel of their homeland located in Canada. Moreover, in our opinion, any such terrorist acts are quite properly described as "activities directed against Canada or detrimental to the security of Canada". It is activity "directed against Canada" in that Canada has a duty under international law, and under domestic statute law, to protect foreign mission property and personnel. A failure to afford reasonable protection is a breach of international and domestic law. Consequently, any conduct directed toward attacking foreign mission premises or personnel is "directed against Canada". It may also be said to be "detrimental to the security of Canada". We think that the legislation should be amended to make it clear that activity of the kind just discussed may be the subject of a warrant authorizing the interception or seizure of communications.

81. It follows from the same opinion by counsel for the Department of Justice that the Solicitor General should not grant a warrant where it is clear that the sole target of foreign terrorists in Canada is against the foreign country on its own territory or at least outside Canada. Again, we think that terrorist activity that is being planned and supported in Canada, regardless of whether it is targetted against Canada or a foreign country, can threaten the security of Canada. The failure to keep such activity under surveillance may disable Canada from discharging its obligations under international agreements to prevent terrorism. The definition of threats to the security of Canada which we shall recommend in Part V as a statutory limit to security intelligence surveillance will cover terrorist activity in Canada against foreign governments.

(iv) *"Foreign"*

82. Doubt exists within the Security Service as to whether the use of the word "foreign" in section 16(3) includes Commonwealth countries. In our opinion, by analogy with Canadian court decisions interpreting other statutes, the word "foreign" does include all other countries, including Commonwealth countries. Should it continue to be felt there is any doubt on this matter the doubt should be resolved by legislation.

83. We have not reviewed all the warrants issued since July 1, 1974, but among those we have considered there are some instances in which it is

difficult to see that the activity of the target person or group was in any way within section 16(2) and (3). Either the police forces or the security intelligence agency (we have doubts as to whether it should be the latter) should be concerned to detect and prevent the activities of such a person and group, in so far as they are directed toward damaging the property of other persons and otherwise violating the Criminal Code and other laws. Yet, we find it difficult to imagine that their activities can properly be described, in any real sense, as "directed toward accomplishing governmental change within Canada".

What does "specify" mean in section 16(4)?

84. A legal question which appears to have gone unnoticed by the Security Service and Solicitors General is that section 16(4)(b) requires the warrant to "specify"

> . . . the person or persons who may make the interception or seizure.

What is the meaning of the word "specify"? No such word is found in section 443, concerning search warrants to be issued by a Justice of the Peace, which provides that the form of warrant shall be directed "to the Peace Officers in the (territorial division)". Section 178.13(2) of the Criminal Code, relating to electronic interceptions of private communications, requires that the authorization "generally describe the manner of interception that may be used" but does not say anything about the person who is to be authorized to make the interception. However, section 178.13(2.1) reads:

> The Solicitor General of Canada or the Attorney General, as the case may be, may delegate a person or persons who may intercept private communications under authorization.

Therefore, neither the provisions for search warrants nor for electronic interception in criminal investigations is of assistance in interpreting section 16(4)(b). The Concise Oxford Dictionary defines the verb "specify" as follows:

> Name expressly, mention definitely.

Webster's New Collegiate Dictionary defines "specify" as follows:

> To name or state explicitly or in detail.

The form of warrant under section 16, prepared by the Department of Justice before July 1, 1974, is directed as follows:

> 2. To the Director General, Security Service, Royal Canadian Mounted Police, and the Members and agents of the Royal Canadian Mounted Police acting under his authority or on his behalf.

We have serious doubts that such a direction complies with the requirement of section 16(4) that the warrant "specify" the person or persons who may make the interception or seizure. Any statutory revision of section 16 should remove this doubt, so as to ensure that the warrants do protect members of the security intelligence agency, and for that matter, that they protect the officials of telephone companies co-operating with the security intelligence agency, who at present may be parties to an interception but cannot be said to be "agents" of the R.C.M.P. acting under the authority of the Director General or on his behalf.

Can a warrant be issued under section 16(2) to intercept or seize written communications?

85. During the first two years of the operation of section 16, the warrants which were issued related to the interception of communications by wiretapping (principally telephonic communications), and by microphone operations (called "oral" communications in the jargon of the Security Service). In 1976, in the investigation of the Omura case, application was made to the Solicitor General for a warrant to authorize the interception of postal communications of a person believed to be associated with Omura. The Solicitor General, Mr. Allmand, signed the warrant but on condition that it not be executed except upon an opinion being received from the Department of Justice that the warrant was valid. On June 14, 1976, the Deputy Minister of Justice, Mr. D.S. Thorson, Q.C., by letter to Mr. Allmand, advised as follows:

> I am of the opinion that the word 'communication' in section 16(2) of the Act includes letters. However, section 43 of the Post Office Act reads as follows:
>
> > 'Notwithstanding anything in any other act or law, nothing is liable to demand, seizure or detention while in the course of post, except as provided in this Act or the regulations. R.S.c.212, s.41.'
>
> In view of the clear wording of the above noted section in the Post Office Act, section 16(2) of the Official Secrets Act cannot, in my opinion, be interpreted as taking precedence over section 43 of the Post Office Act.

For present purposes, the significant portion of Mr. Thorson's letter is his one sentence opinion that the word "communication" in section 16(2) of the Official Secrets Act includes letters. In consequence, one warrant was obtained in May 1976, authorizing the interception of "written communications" of a target organization. Mr. Tassé testified that early in 1977, while he was still Deputy Solicitor General, a further opinion, this time verbal, was obtained from the Department of Justice that section 16 authorized the interception or seizure of "written" communications (Vol. 156, p. 23814). Later in 1977, having become Deputy Minister of Justice, Mr. Tassé signed a written opinion to the same effect. Consequently, since then the Security Service and the successive Solicitors General have considered section 16 to authorize the issuing of warrants to intercept and seize "written communications". In our view, there is a serious question as to whether section 16(2) authorizes the issuing of a warrant to intercept or seize "written communications". The amendment to the Official Secrets Act in 1973 was part of the Protection of Privacy Act, the principal provision of which made it an offence to "wilfully intercept a private communication. . . by means of an electromagnetic, accoustic, mechanical or other device". The provisions of the amendment to the Official Secrets Act must be read in the context of the Protection of Privacy Act as a whole unless there is some indication in the statute that the Official Secrets Act amendment is to be read differently. As was said by Mr. Justice McIntyre in the Supreme Court of Canada:

> It was said that well-established canons of construction dictated that words should receive a uniform meaning when used repeatedly in the same statute or in one *in pari materia*. Following this principle, it was said, the separate

> parts of the Protection of Privacy Act which amended the Criminal Code, the Crown Liability Act and the Official Secrets Act, respectively, should be construed as a unified whole, providing one body of law applying to the separate situations covered by the separate Acts which were amended. I have no quarrel with the general proposition thus expressed...[32]

The amendment to the Official Secrets Act created an exception to the criminal liability imposed by the principal part of the Protection of Privacy Act:

> 16. (1) Part IV.1 of the Criminal Code does not apply to any person who makes an interception pursuant to a warrant. . .

This does not mean that one can read section 16 without regard to the provisions of Part IV.1 of the Criminal Code, for both provisions formed part of the Protection of Privacy Act. Moreover, unless there is language leading to a contrary construction, the language of section 16(1) and (2) must be read as providing a defence to what section 178 of the Criminal Code makes an offence, and sections 16(1) and (2) must not be read as providing a statutory procedure for authorizing something which is otherwise no offence under section 178. Thus "communication" as used in section 16(2), not being defined in the amendment to the Official Secrets Act, must be given the same meaning as in the remainder of the Protection of Privacy Act. In the principal part of the Protection of Privacy Act, which enacted section 178 of the Criminal Code, the word "communication" is defined only as part of the definition of the expression "private communication". Part of the definition of that expression in section 178.1 reads:

> Any oral communication or any telecommunication. . .

(The balance of the definition relates to the word "private", which has no relevance to section 16 of the Official Secrets Act.) There is only one respect in which section 16(2) may contain an indication that it is meant to apply to communications of a broader or different kind than those with which the balance of the Protection of Privacy Act was concerned: the word "seizure" may imply that written communications are included within the purview of section 16(2). However, we doubt that that element overcomes the reasoning previously stated. Thus, in our opinion, it is at least doubtful that section 16(2) of the Official Secrets Act can be read as authorizing the Solicitor General to issue a warrant in respect of written communications of any kind, whether letters in the post or other written communications (other than telegraphs, cables and telexes, which would be "telecommunications"). Therefore, if there is to be legislation permitting the opening of mail for security purposes, section 16 of the Official Secrets Act would have to be amended further than needed merely to provide that its provisions override the provisions of the Post Office Act; section 16 would have to contain language redefining "communication". Moreover, if section 16 is to be taken as authority for the issuing of warrants for the seizure or copying or photographing of some forms of written communication in the course of post, other than letters, (e.g. printed books, typed books, accounting records and code books), which may not properly be described as

[32] *Goldman* v. *Regina* (1980) 51 C.C.C. (2d) 1 at 19; 13 C.R. (3d) 228 at 251.

"communications", the legislation should be amended to empower the Solicitor General to issue a warrant authorizing such acts. It follows from our reasoning that if the Bill introduced in Parliament in January 1978 had been enacted, it would not have achieved its intended purpose.

Use of section 16 warrants for purposes of search

86. After July 1, 1974, the Security Service was concerned as to the means by which it should gain approval for "PUMA" operations, that is, operations involving surreptitious entry upon premises to search and examine articles on the premises and copy or photograph them. In the early period of the operation of section 16, the Security Service considered that the use of warrants issued by the Solicitor General authorizing the interception of oral communications was an umbrella for PUMA operations which was "not entirely appropriate but better than nothing". In two cases the Security Service applied for warrants under section 16 under the representation that the interception or seizure of the targetted individual or group's communications was necessary for the prevention or detection of subversive activity, when the real intention and sole object of the Security Service was not to intercept oral communications but rather to search, examine, copy and photograph articles found on the premises where the electronic device was to be installed. We are not suggesting any impropriety in these two cases; the members involved in preparing the applications thought that they were following the proper procedure for obtaining authority for such a search. Other than these two cases, it can be said that the Security Service considered that where it could find the grounds to support a genuine application under section 16, it was then consciously prepared, when entering the premises to install a listening device, to have its members seize the opportunity to search, examine, copy and photograph. This continues to be the approach of the Security Service. Whether this is a lawful practice has already been discussed under the title "Rummaging", earlier in this chapter.

Use of information obtained through warrants issued under section 16

87. There is a deficiency in section 16 of the Official Secrets Act from the point of view of providing protection for members of the Security Service who communicate the content or purport of a communication intercepted under a section 16 warrant to a friendly foreign agency. For example, one may reasonably expect information obtained by our security intelligence agency about an international terrorist, who is in Canada, to be transmitted to the agency of another country which shares Canadian concerns about the person's future activities. If the Canadian security intelligence agency does not provide information it has of that nature to friendly agencies, they in turn are unlikely to give the Canadian agency information they have that may be of interest to Canada. Reciprocity is expected. If the information has been obtained as a result of electronic interception of communications, there may be a serious legal problem in this action. It arises from section 178.2(1) of the Criminal Code, which prohibits the wilful use or disclosure of a private communication "or any part thereof or the substance, meaning or purport thereof or of any part thereof" without the consent of one of the parties to the communication;

but subsection (2) provides that that does not apply to a person who makes any such disclosure

(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;

(c) in giving notice under section 178.16 or furnishing further particulars pursuant to an order under section 178.17;

(d) in the course of the operation of

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

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

if the disclosure is necessarily incidental to an interception described in paragraph 178.11(2)(c) or (d); or

(e) where disclosure is made to a peace officer and is intended to be in the interests of the administration of justice.

None of these exceptions appears to protect a member of the R.C.M.P. Security Service who discloses such information to the security intelligence agency of another country. We shall recommend that statutory protection be extended to such an employee of the security intelligence agency. (See Part V, Chapter 4.)

88. There is legal protection for the employee of the Security Service who listens to the intercepted communication and translates or transcribes it, because section 16(1) of the Official Secrets Act says that Part IV of the Code does not apply to a person who makes an interception pursuant to a warrant or to any person who aids him. However, what about the employee or member of the Security Service to whom the transcript is delivered, who then analyses it and condenses it into a report which is placed on file for other members to read or which is transmitted to other members or even to other departments of the government? None of the exceptions contained in section 178.2(1) affords protection to him. Nor does section 16(1) of the Official Secrets Act afford protection, for it cannot be said that any of those persons are persons who "in any way" aid the person making the interception. Consequently we shall recommend that protection be afforded to such persons by amendment to section 16, when disclosure is made to any person for the purposes of carrying out the functions of the security intelligence agency and subject to strict guidelines about reporting security intelligence. (See Part V, Chapter 4.)

Miscellaneous legal issues arising from the technical aspects of electronic surveillance

89. There are a number of legal issues that require resolution if the security intelligence organization is to be able to carry out its responsibilities once a warrant is issued authorizing electronic interception of communications.

90. The R.C.M.P. identified as a problem the possibility that radio transmitters installed pursuant to a warrant issued under section 16 of the Official Secrets Act might violate the licensing requirements of the Radio Act. That problem was resolved in 1979 when the Minister responsible under the Radio Act granted a blanket licence for the use of "any and all types of radio apparatus to be used by persons acting under the direction of the Director General of the Security Service in the course of investigations related to national security matters, which radio apparatus is of a special design for which the prescribed procedures for technical approval and acceptance are not appropriate". Such a licence is permissible under section 4(1)(b) of the Radio Act. Thus, while there no longer is a legal problem, we note that until 1979 microphone operations may have violated the provisions of the Radio Act.

91. Another concern is that members of the R.C.M.P. engaged in making the technical installation may be violating the requirements of provincial laws regulating the qualifications of persons making electrical installations. (The problem presumably exists also in the case of installations made in the course of criminal investigations under section 178 of the Criminal Code.) A similar problem arises when the Security Service makes a major electrical installation in its own premises, whether at Headquarters or elsewhere across the country — for example, for the reception of electronically eavesdropped conversations. The Security Service does not have personnel who meet the residency requirements of all the provinces. The use of contracted personnel bears inherent security risks. Apart from accepting such risks and contracting with outside personnel, we can recommend no other course but to negotiate lawful administrative arrangements with the provincial authorities and, if necessary, request exemptive provincial legislation to cover the specific need. We realize that this problem, and the problem discussed in the next two paragraphs, may in law be non-existent if a correct interpretation of the judicial decisions on the Constitution would lead to the conclusion that such works and undertakings by the R.C.M.P. would not be subject to provincial regulatory laws. However, the answer to that question, short of going to court for a ruling, must remain uncertain. Therefore we think it best that it be assumed that provincial law is applicable and that negotiations with the provincial authorities be carried out.

92. Another concern is that the installation of equipment in 'observation posts' and 'listening posts' — houses, apartments and offices from which to observe actions and receive intercepted communications at nearby targetted premises — may violate provincial and municipal laws, such as fire regulations. The Security Service wishes to avoid having to comply with such regulations because compliance, meaning permits and inspections, might endanger the security of such operations. Moreover, the nature of the installation is frequently such that the security intelligence organization will be unable to meet the minimum provincial or municipal standards of protection. We can see no alternative but to ask provincial governments to amend relevant statutes to exempt such installations. In the specific case of fire regulations, for example, the standards of protection should be inspected in all such posts by an inspector of the office of the Dominion Fire Commissioner. There is already an inspector in that office who has the requisite security clearance and inspects restricted areas in buildings owned by the R.C.M.P. Security Service.

93. A similar concern is that provincial and municipal building codes may be violated by structural alterations that may have to be made to premises used as observation posts or listening posts. This may consist of the construction of false walls, modifications to plumbing, etc. Applications for permits and examination by provincial or municipal inspectors would endanger the security of the operation. We doubt that many of the alterations to premises required by such operations would constitute such 'construction' or 'demolition' of a 'building' as would violate the typical provincial statute which prohibits such construction without a permit, or would constitute violation of the typical provincial statute which prohibits a 'material change' in a plan on the basis of which a permit was issued without satisfying the authorities. Nevertheless, because of the possibility that violations might occur, we think that provincial governments should be asked to amend building code legislation to exempt such alterations provided that they do not weaken the structure of, or otherwise endanger, a building, or result in an occupant being subjected to an unreasonable danger.

94. Another concern is that sometimes the method of eavesdropping, when authorized under section 16 of the Official Secrets Act, is by means not of a wire microphone or a battery-operated radio transmitter but by a transmitter which is powered by the power supply paid for by the subject of investigation or another person. This may constitute an offence under section 287 of the Criminal Code, which provides as follows:

> 287. (1) Every one commits theft who fraudulently, maliciously, or without colour of right, (a) abstracts, consumes or uses electricity or gas or causes it to be wasted or diverted. . .

It might be argued that the Solicitor General's warrant gave the accused a "colour of right" — i.e. a belief that he had a right to take "possession" of the electricity for the purposes of the authorized interception — although we do not subscribe to the validity of such an argument. To remove the lingering concern, we shall recommend that the amendments to the legislation expressly empower the use of devices that operate by using the electrical power supply found upon the premises. We are advised that the value of the amount of power thus used is a matter of cents per month, and we do not consider the burden thus placed upon the suspect or neighbour to be significant. (The same solution should apply on the side of criminal investigations, to section 178 of the Criminal Code.)

Importing highly sensitive equipment

95. Occasionally the Security Service, wishes to bring into Canada novel and effective surveillance equipment, designed to detect communications and observe conduct, which it would be too costly to manufacture in Canada. On these occasions, the Security Service is properly concerned to reduce to a minimum the number of people who know of the existence of this means of detection and its capabilities. Therefore the Security Service has wished to avoid inspection of such items by customs officers.

96. The Customs Act contains no provisions exempting any goods imported into Canada from being examined by the Customs and Excise Branch. In fact,

in the case of another federal government department, military equipment is imported without inspection by virtue of an arrangement under which the customs officer is instructed not to inspect the goods. However, we believe that a better and firmer solution should be found. An administrative solution that would be preferable would see one Customs inspector being given the requisite security clearance to attend to all such imports. If that should prove unworkable, we consider that the legislation chartering the security intelligence organization should expressly exempt from the provisions of the Customs Act such equipment as may be required by the organization for its purposes, such requirement to be certified by a certificate of the Director General attached to the particular goods.

Does the Diplomatic and Consular Privileges and Immunities Act raise any impediment to a Canadian security intelligence agency's work in countering espionage?

97. The Vienna Conventions on Diplomatic and Consular Relations were signed by Canada on February 5, 1962, and have been part of Canadian domestic law since June 29, 1977, as a result of the enactment of the Diplomatic and Consular Privileges and Immunities Act. Section 2(1) of the Act states that certain Articles of the Vienna Convention on Diplomatic Relations and of the Vienna Convention on Consular Relations "have the force of law in Canada in respect of all countries (including Commonwealth countries), whether or not a party to the conventions." The provisions of the two Conventions are substantially the same. Reference will be made only to the Convention on Diplomatic Relations. The following are articles from that Convention which, in the schedule to the Act, have the force of law in Canada:[33]

> 22.1. The premises of the mission shall be inviolable. Agents of the receiving State may not enter them, except with the consent of the head of the mission.
>
> 2. The receiving State is under a special duty to take all appropriate steps to protect the premises of the mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity.
>
> 27.1. The receiving State shall permit and protect free communication on the part of the mission for all official purposes. In communicating with the Government and the other missions and consulates of the sending State, wherever situated, the mission may employ all appropriate means, including diplomatic couriers and messages in code or cipher. However, the mission may install and use a wireless transmitter only with the consent of the receiving State.
>
> 2. The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions.

98. The following legal issues have been raised:

(a) Is it Canadian law that a violation of the provisions of Articles 22 and 27 of the convention occurs if the telephone lines of a foreign mission

[33] S.C. 1976-77, ch. 31.

were to be tapped or a listening device were to be installed and used in the premises of a foreign mission?

(b) Is it Canadian law that a violation of the provisions of the convention occurs if the security intelligence agency were to have a human source inside a foreign mission?

(c) Is it Canadian law that a violation of the provisions of the convention occurs if the security intelligence agency were to have a member or other person enter the premises of a foreign mission, under a pretext?

99. Some introductory remarks are in order, concerning customary international law, the Conventions and the statute. In customary international law, the inviolability of diplomatic premises has long been recognized as subject to the overriding principle that the embassy must not be used to the detriment of the host country or for the purpose of infringing the law of that country. The best known example of not accepting the inviolability as absolute arose in 1896, when the British Government announced its intention to invade the Chinese embassy in London in order to rescue Sun Yat-Sen, who was being held in the embassy against his will with the object of sending him back to China. The purpose of a mission is to represent the views of its country to the host state. The mission is not entitled to engage in espionage or endanger the security of the host state. Nor is the host state required to tolerate activities by the mission which go beyond its proper function. The host state is entitled to take such measures as are necessary to preserve its own security. If the mission abuses its rights, the host state is entitled to take measures to counter such activities, so long as they remain proportionate in character. The foregoing principles however, do not provide guidance on the key question of the rights of the host state when it comes to the acquiring of information concerning the possibility of violations of diplomatic privileges and immunities. We are, however, persuaded that the host state has a right to acquire knowledge of whether the persons who enjoy the privileges and immunities recognized by the Convention are violating their own duty not to interfere in the affairs of the host state. It therefore follows that the host state has the right to take reasonable steps to acquire such knowledge.

100. While normally a treaty would be regarded as overriding the principles of customary law, this is true only when the treaty is a law-making document. In the case of the Convention, the purpose was to codify what were regarded as being the customary and accepted rules on the subject, and to provide some text which would be acceptable to the new states, many of which have contended that there is no true customary law in existence, since what is described as being such law came into being before the creation of those states and without their consent. To this extent, therefore, in so far as the text of the Convention does not expressly overrule accepted rules of customary law, these are considered to be still in existence. The Convention is confirmatory of international customary law and to the extent that it does not expressly override such law it leaves it intact (see, for example, *The Amazone*[34]).

[34] [1940] P. 40. This case referred to the Diplomatic Privileges Act, 1708, as being declaratory and not exhaustive of diplomatic privileges, so that in so far as the Act was silent the privileges of customary law still existed.

Secondly, when codificatory instruments are being drafted it is not the practice to list all the exceptions and waiver possibilities, particularly when state practice over the centuries has recognized the possibility of even the invasion of an embassy.

101. It cannot be presumed that Parliament intended to legislate in a way that would inhibit protective action, especially as such action is compatible with the principles of customary international law concerning diplomatic privileges and immunities. The statute is principally concerned with acts taken by private individuals, which may contravene the rights of diplomatic missions, and not acts by state agents or on behalf of the state. It does nothing more than to give modern legislative form to what has been the position under customary law, both national and international, with regard to the protection of diplomats. The obligation upon the receiving state to protect the mission from intrusion and the like relates to the activities of private interests and does not create any criminal liability in respect of acts interfering with the mission's security undertaken by or on behalf of the host state.

102. The purposes of the inviolability provisions of Article 22 are to enable the mission to function peacefully and without interference, to prevent the host state from inhibiting such activities by unwarranted interference, and to secure the mission from illegal activities by local residents. The aim is to enable the mission to carry out its proper activities (which are set forth in Article 3 of the Convention).

103. Article 22 does not protect the mission in so far as the mission goes beyond the purposes for which it had been accepted. Article 41.1 forbids interference in the internal affairs of the host state, and Article 41.3 forbids use of the premises of the mission "in any manner incompatible with the functions of the mission as laid down in the present convention or by other rules of general international law or by any special agreements in force between the sending and the receiving State." Thus, if an embassy were being used as a "prison" for nationals of either the host or the sending country, the mission would be violating the provisions of Article 41.1 and 41.3, and Article 22, the purpose of which is to enable the mission to perform its proper functions peacefully and without interference. The purpose of those articles is not to preclude the local authorities from entering the embassy.

104. As far as telephonic communications to and from the mission are concerned, if they concern activities which are beyond the proper activities of the mission, by the same reasoning Article 27 would not be violated by the host state taking steps to detect such communications. In any event, provided that the steps taken to "wiretap" occur outside the mission premises, there is no question of a violation of such premises. Moreover, as far as Article 27 is concerned, such listening does not obstruct or inhibit "free communication on the part of the mission for all official purposes".

105. If the electronic surveillance is by a microphone installed in the premises, where the host state has grounds for suspecting activities on the part of the mission beyond the appropriate functions of the mission, in our view there is no violation of either Article 22 or Article 27.

106. Nor, in our view, does Article 22 prevent the security intelligence agency of the host state from having a human source inside the mission, or from having a person enter the mission premises under a pretext. When Article 22 refers to entry, there is little doubt that the draftsmen had in mind a physical invasion. They were concerned with enabling the officers of the mission to fulfill their tasks without threats or fears of bodily harm by local nationals invading the premises. Article 22 does not preclude the host state taking measures of anticipatory self-defence, for example by obtaining information as to whether there has been an abuse of the mission's functions.

107. Our conclusion is that the use of certain investigative techniques, when there are grounds to suspect that the mission's staff is engaged in espionage, would not result in an offence being committed under section 115 of the Criminal Code, for there is a "lawful excuse" for such conduct. Moreover, persons involved in such conduct in the course of the investigation of suspected espionage could not be said to be "wilfully" omitting to do anything which is required to be done by any of the articles of the Diplomatic and Consular Privileges and Immunities Act.

(c) *Legal and policy issues unique to the C.I.B.*

108. The 1979 Annual Report prepared by the Solicitor General of Canada and laid before Parliament in 1980, pursuant to section 178.22 of the Criminal Code noted somewhat obscurely that the following was an area of concern:

> The provisions regarding the disclosure of information by electronic surveillance. These provisions impede rather than facilitate international exchanges of information.

This no doubt is a reference to a problem that the R.C.M.P. has drawn to our attention as to whether members of the R.C.M.P. may give to a foreign law enforcement agency any information which the R.C.M.P. obtains from electronic surveillance. In the discussion of legal and policy issues concerning the Security Service we have mentioned the offence created by section 178.2(1) of the Criminal Code for disclosure of the content or purport of a communication, and the exceptions provided by subsection (2). None of these exceptions appears to protect a member of the R.C.M.P. who discloses such information to a foreign agency, unless it can be said that (e) is applicable, which is doubtful. We shall recommend that section 178.2(1) be amended to make it clear that such information may lawfully be given to a foreign law enforcement agency.

109. Another aspect of the limited exceptions is that members of the R.C.M.P. are severely restricted as to what information they may give to anyone involved in the preparation of the Annual Reports of the Solicitor General of Canada and the provincial attorneys general. Consequently the Annual Reports are likely to be less informative than they should be as to the value of the intelligence product received, unless evidence adduced in court has resulted. This limitation equally would severely impede any attempt in the future, whether within the R.C.M.P. or by any other body, to conduct an assessment of the benefits of electronic surveillance in comparison with the tangible and intangible costs of such operations. We shall recommend that

section 178.2(1) be amended to make it clear that such information may lawfully be given to any person, whether that person is a peace officer or not, who is involved in the preparation of the Annual Reports.

110. Our examination of the operation of section 178 of the Criminal Code has been limited to consideration of the procedure by which applications are made to a judge for an authorization. We did not think that consideration of the entirety of section 178 was within our terms of reference. For there have been no suggestions made to us that in some respect the R.C.M.P. has been using section 178 in a way that is "not authorized or provided for by law"; consequently consideration of section 178 as a whole would not fall within paragraph (a) of our terms of reference. Nor does it fall within paragraph (c), for section 178 has not in practice been used as a means of obtaining authority for the Security Service to conduct electronic interception of communications. However, we did address our attention to the application procedure because we wanted to have a good grasp of how it is functioning, in case some aspect of the procedure would have a bearing on the procedure that might be used if the law is amended to permit the opening of mail for purposes of any criminal investigations, a subject that was certainly within the terms of reference because of past practices "not authorized or provided for by law". Whatever our recommendation might be in that regard, we knew that the Bill introduced in Parliament in January 1978 proposed that the procedure by which an application for judicial authorization would be made should be akin to that already provided for in the case of electronic interception. Therefore it seemed to us that it was important to examine the existing application procedures.

111. However, this was not an easy task. Section 178.14 of the Criminal Code requires all documents relating to an application to be treated as confidential. Further, all the documents except the authorization itself are required to be placed in a packet and sealed by the judge. The packet is to be kept in the custody of the court and is not to be opened except for the purpose of dealing with an application for renewal of the authorization, or pursuant to an order of a judge. An application was made on behalf of a provincial judicial inquiry for an order to open a packet so that the inquiry might examine the affidavit, but the Chief Justice of the Trial Division of the Supreme Court of Alberta refused to make the order sought.[35] Thus it is apparent that at present the Code does not permit a Commission of Inquiry to gain access to affidavits sealed in packets, to examine the quality of the documentation filed in support of authorizations that have been given. Moreover, to comply with the spirit of section 178.14, the Department of Justice and the R.C.M.P. do not retain copies of the applications once the authorization has been granted. So, even if the Department were prepared to give us access to such documents, they are simply not available for inspection. While on the one hand the law and the administrative practice thus genuinely further the statutory objective of confidentiality, on the other hand they render it impossible to assess the quality of the documentation other than by questioning some of those who since 1974 have been involved in the application process. This we have done, and while so

[35] *Re Royal Commission Inquiry into the Activities of Royal American Shows Inc. (No. 3)*, (1978) 40 C.C.C. (2d) 212.

doing we have explored with them the workings of the application procedure. The constraints we have encountered in this regard have alerted us to the impossibility under the present law of any thorough review of the quality of the documentation which is prepared by agents of the Solicitor General — or, for that matter, of the provincial attorneys general. Similarly, the prohibition against disclosure of the content or purport of an intercepted communication, found in section 178.2, has exceptions (such as the giving of evidence in court, or for the purpose of a criminal investigation, or where disclosure is made to a peace officer and is intended to be in the interests of the administration of justice), but they would not permit any independent review of the benefits of interceptions compared with the expectations described in the affidavits. In Part X, Chapter 5 we shall make a recommendation concerning independent review of the authorization procedure, and we shall recommend an amendment to section 178 to permit that review process to have access to the information it would need.

E. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

112. In this Chapter we have, in the course of giving the history and discussing the legal issues, recognized the need for the use of electronic surveillance in both security intelligence collection and criminal investigations. We have also pointed to a number of deficiencies in the law which will be the subject of recommendations in Part V, Chapter 4 and Part X, Chapter 5.

CHAPTER 4

MAIL CHECK OPERATIONS — SECURITY SERVICE AND C.I.B.

A. ORIGIN AND NATURE OF PRACTICE — SECURITY SERVICE AND C.I.B.

1. Research carried out by us discloses that the interception of mail was a matter of concern at least as early as the 1914-18 war. The War Measures Act included a prohibition against dissemination of treasonable material or the passing of information to the enemy. At the beginning of the war a number of postmasters were simply handing over any mail they considered suspicious to the then Royal North-West Mounted Police. It was soon realized that more proper authorization was required and warrants were then obtained under what was then section 629 (now section 443) of the Criminal Code — the section that provides for a search warrant being issued by a justice of the peace. The Post Office Department objected that this was contrary to what was then section 84 of the Post Office Act. The problem was resolved by the senior law officers of the Crown directing that in cases of suspicion the police were to contact senior authorities at the Post Office who would make the necessary arrangements in a proper case. This pragmatic solution continued for some time after the war.

2. The question again became important just prior to the 1939-45 war. By this time the Intelligence Section of the R.C.M.P. had been formed. In early 1939, at about the time the Official Secrets Act was being introduced with a view to meeting the anticipated problem of espionage activity, the Force suggested that the Post Office Act should be amended to permit mail examination in order to counter suspected espionage. Consideration of this suggestion was shelved when the war commenced and the Defence of Canada Regulations brought postal censorship into effect. This solution lasted until the expiry of the regulations in 1954.

3. In late 1954 correspondence and discussions took place between the Force and the Department of Justice with a view to regularizing covert inspection of mail. The Security and Intelligence Special Branch of the R.C.M.P. considered such inspection necessary for security reasons. The possibility of using warrants under section 11 of the Official Secrets Act was considered in view of the fact that the offence created by section 55 (now section 58) of the Post Office Act applied only to a "person who *unlawfully* opens... any post letter, or other article of mail...". At the time, however, it was pointed out that in 1950 section

41 (now section 43[1]) had been introduced into the Post Office Act. It provided as follows:

> Notwithstanding anything in any other Act or law, nothing is liable to demand seizure or detention while in the course of the post, except as provided in this Act or the Regulations.

Consideration was given to amending the Post Office regulations to permit covert examination of mail but nothing came of this suggestion.

4. In October 1957, the Report to the Prime Minister of the Committee of Privy Councillors Appointed to Inquire Into the Interception of Communications[2] (the Birkett Report) (Ex. B-14) was published in the United Kingdom. This report examined the legal authority for the interception of mail, telegraph and telephone communications as well as the purpose, use and extent of the power to intercept, and it made recommendations for the future use of the power. In the United Kingdom all three methods of communication were in fact services provided by the Post Office. The Birkett Committee found that, although apparently originally based upon Crown prerogative, the power to intercept communications in the course of post had been recognized by statute in the U.K. for more than 200 years. Prohibitions similar to that found in section 43 of the Canada Post Office Act had been subject to express exception from 1710 onwards, permitting the interception of mail and, later telegraph on the basis of a warrant of a Secretary of State. The Committee recommended a clarification of the statutes regarding the power to intercept telephone communications. Upon reviewing the use of the power to intercept, the Committee concluded that it had been effective and, subject to continued safeguards, should be continued, since the interference with the individual liberty of law-abiding citizens was relatively small.

5. In Canada, on March 1, 1962, the Director of Administration of the Post Office issued a Directive, addressed to the Regional and District Directors and Senior Investigators, entitled "Narcotics in the Mails" (Ex. B-49). It directed that the Post Office should extend every possible co-operation to the R.C.M.P. in their drug investigations despite the fact that the newly enacted Narcotics Control Act did not override the Post Office Act, which provided (and still provides), that nothing is liable to demand, seizure or detention while in the course of post. The procedure to be followed was not set out but rather left to the discretion of senior officers in the field. The existence of mail suspected of containing narcotics was to be communicated to investigating police in such a way as to inform them of "the precise method, time and place of its delivery to the addressee or of its return to the sender". The co-operation of Customs was to be enlisted in the case of international mail. It was also specified that those in the field did not need to report to Headquarters.

6. This Directive was withdrawn in 1972, when the Department was reorganized on a regional basis, and was subsequently replaced by a Directive dated January 14, 1974, sent by Mr. P. Boisvert to the four Regional Chief

---

[1] R.S.C. 1970, ch.P-14.

[2] Cmnd. 283.

Inspectors of Security and Investigations (Ex. B-51). This Directive specified that because of section 43 of the Post Office Act and other factors, inquiries from R.C.M.P. Drug Enforcement Branch personnel should be directed to Security and Investigations personnel, preferably postal inspectors, rather than the regular Post Office operational staffs. The postal inspectors were briefed on this subject at a postal inspectors' training course held in October 1973, and the issue of special relations with the Post Office was to be included in training courses of R.C.M.P. Drug Enforcement Branch personnel. The January 14, 1974 Directive, and the understanding contained therein, was renewed in an exchange of correspondence dated April 1, 1977 and subsequently confirmed again by letter of January 6, 1978 from Mr. Boisvert to this Commission.

7. Mr. Boisvert told us that it was his clear understanding that any mail cover check operation (that is, the examination of only the outside of a piece of mail) would be done (a) in the Post Office and (b) without removing the piece of mail from the post office where it was located.

8. Documents before the Commission indicate that consideration was given in 1973 to expanding the Protection of Privacy Bill to include specifically the interception of communications by mail. Nothing, however, came of this suggestion.

9. The escalation of drug trafficking in the late 1960s and early 1970s made the criminal investigations side of the Force more anxious to secure legal authority to open mail. Interdepartmental meetings at the instance of the R.C.M.P. began in 1974 with a view to securing appropriate amendments to the Post Office Act.

10. In the summer of 1976, the Security Service attempted to secure access to first-class mail under a warrant which was issued by Mr. Allmand pursuant to section 16 of the Official Secrets Act. He issued the warrant subject to receipt by the Security Service of an opinion that such a warrant was legal. Having been advised by the Department of Justice that section 43 precluded the exercise of such a warrant, the Security Service joined the C.I.B. in seeking amendments to the Post Office Act.

11. Legislation patterned upon the Protection of Privacy Act, which would have amended the Criminal Code, the Crown Liability Act and the Post Office Act, was introduced as Bill C-26 on February 7, 1978, while our hearings relating to Mail Check Operations were underway. This proposed legislation provided for its automatic termination one year after the publishing in the House of Commons of the final Report of this Commission. The Bill perished with the prorogation of Parliament in May 1979, and has not been re-introduced.

B. R.C.M.P. POLICIES AND PROCEDURES — SECURITY SERVICE AND C.I.B.

(a) *Security Service*

12. Although it is apparent from the record before us that mail check operations under the code name CATHEDRAL were carried out by members

of the Security Service from the demise of the Defence of Canada Regulations in 1954, the investigation and evidence before us concentrated on the period from 1970 onward. The principal reason for adopting this time period was that before November 2, 1970, decisions with respect to the use of mail check operations were made by area commanders at the division level, and no records were kept at Headquarters.

13. On November 2, 1970, a senior R.C.M.P. officer sent a memorandum to the commanding officers of the various area commands of the Security Service. The memorandum describes the three types of CATHEDRAL coverage as follows:

> *CATHEDRAL "A" — Routine name or address check* (It was explained in evidence that in this instance, a member of the R.C.M.P. asked a postal employee to record in longhand the name of the addressee and any information with respect to the sender by looking at the outside of envelopes.)
>
> *CATHEDRAL "B" — Intercept (photograph or otherwise scrutinize by investigator) but do NOT open*
>
> (In this instance the same procedure was followed as that in Cathedral "A" but a photographic copy was made of the outside of the envelope. It was explained in evidence that this procedure was used to examine mail covers for simple codes and the possible presence of micro-dots.)
>
> *CATHEDRAL "C" — Intercept and attempt content examination*

14. With respect to authorizing such operations the memorandum directed that Cathedral "A" and Cathedral "B" could be authorized by the local officer in charge, Security and Intelligence Branch, or his designee, but continued: "Because of the special experience required to handle a Cathedral "C" and for this reason only the D.S.I.'s authorization for an operation will henceforth be required. This authority will be contingent on the importance of the case and the availability of a trained technician". The reason given for this change in authorization procedure shows a very clear understanding on the part of the senior officers at Headquarters as to the legality of such techniques. The first two paragraphs of the memorandum read as follows:

> *Re: CATHEDRAL*
>
> It has become apparent that considerable diversity exists in the understanding and the utilization of this source and that we are unconsciously exposing this source's availability to unwarranted risk. Since this source is extremely valuable, perhaps in regard to counter-espionage particularly, it has been decided that there should be some uniformity brought into the picture by outlining guidelines which will create as few restrictions and limitations as possible and still effectively reduce the risk.
>
> It must be clearly understood that any form of co-operation received from any CATHEDRAL source is contrary to existing regulations. There is absolutely no indication that this aspect is likely to be rectified in the near future. Since these investigations involve National Security, it is considered there is a sufficient element of justification to proceed with the development and cultivation of sources who are willing to co-operate on this basis. Each source who co-operates with the Force is actually risking his livelihood and

this fact must be kept in mind when the individual is being recruited or subsequently handled.

Directions were given in the memorandum as to co-ordinating and supervising the operation at each of the divisions. Concern was expressed that all approaches to Post Office personnel should be co-ordinated and that liaison should be maintained between the Security Branch and the C.I.B. "to ensure there is no conflict".

15. It may be noted that, although from late 1970 onward policy required that all Cathedral "C" Operations be approved by Headquarters, there were Cathedral "C" operations in nine cases from 1971 to 1976, without approval having been obtained (Ex. B-31).

16. A former senior R.C.M.P. officer testified that Cathedral "C" was in fact used in cases of counter-terrorism, counter-espionage and later to protect persons against letter bombs. He knew of no other areas of activity in which authorizations were granted in the Security Service for a Cathedral "C" operation.

17. In the late spring of 1973 an incident occurred in connection with mail service which caused an addressee to communicate with Members of Parliament regarding the opening of mail. Because Headquarters was concerned that this might result in public revelation of the Cathedral operations, a message was sent on June 22, 1973 (Ex. B-17), to all Area Commanders which directed that:

> All Cathedral "A", "B", and "C" operations are to be suspended until further notice. No further operations are to be instituted until you are advised the suspension is lifted.

18. No record or instruction has been found to indicate that there was ever a formal revocation of the suspension of Cathedral operations directed in the telex of June 22, 1973. However, subsequent evidence (*in camera*) indicates that one Cathedral "C" operation was authorized in September 1973 and a number were approved in 1974 (Exs. BC-2, BC-3, and B-31).

19. Assistant Commissioner M.S. Sexsmith was in security and intelligence work in the R.C.M.P. from 1958 until January 1978. In May 1973, he was the Area Commander of the Security Service in Toronto. In August 1975, he became Deputy Director General (Operations). He indicated to us that upon his appointment as "D.D.G. Ops" he adopted a policy pursuant to which he had not seen fit to authorize any Cathedral "C" operations. The reasons given by him for not authorizing any Cathedral "C" operation from the time of his appointment on August 1, 1975 may be summarized as follows:

(a) The American experience with Watergate and the suspicion of the media in Canada that there was a Watergate in this country might lead to disclosure of the mail examinations and interceptions and thus cause damage to the Security Service.

(b) Some former members of the R.C.M.P. were beginning to talk to the media and "other people".

(c) Several initiatives over a long period of time to have the law amended so that the mail could be opened legally "under strict control" had failed and it seemed, to Mr. Sexsmith, to be unfair in the circumstances to ask members of the R.C.M.P. "to stick their necks out and open mail".

20. An incident involving a mail-cover check in the Hamilton area first came to public attention on November 8, 1976, when Mr. Paul Boisvert, Director of Security and Investigations in the Post Office, received information from the Postmaster General's Office to the effect that a complaint had been received concerning a mail check in Hamilton. Mr. Boisvert immediately telephoned the Regional Chief of Security and Investigations and requested him to conduct an investigation. The investigation disclosed that on or about October 4, 1976, a postal inspector in Toronto received a request from the R.C.M.P. to implement a mail-cover check on a subject living in Hamilton. The Toronto postal inspector sent a memo to the manager of the Hamilton post office requesting that mail addressed to the subject be sent under registered cover to the Toronto unit.

21. "Approximately 30 pieces of sealed letter mail" were received by the postal inspector in Toronto, where these letters were photostated and returned the same day, again under registered cover, to the Hamilton post office. None of the envelopes was opened or left the custody of the Post Office (Vol. 17, p. 2638). In one case the postal inspector remembered one small sealed envelope having arrived at the Toronto office repaired with scotch tape on the centre of the cover. According to the postal inspector this was returned in the identical condition.

22. The postal inspector added in his report to the Chief Postal Inspector of the Ontario postal region that in the past he had complied with similar confidential requests "placed with (his) unit, by special law enforcement squads". He further pointed out that this type of co-operation was suggested in his Investigator's Manual, and that the R.C.M.P. officers involved in the matter never took possession of the mail, did not open or damage any articles, and did not disclose the purpose of the investigation.

23. Mr. Boisvert met with the Postmaster General on November 16, 1976 at which time he assured the Minister that "this was an isolated incident that was improperly handled by the postal inspector who was due to retire next month". However, he was satisfied that "the mail never left the custody of the Post Office", and, further, that he had met with senior officials of the Royal Canadian Mounted Police who assured him "that they did not come into possession of the mail as for their purpose they were satisfied with the photocopies of the outside of the envelopes only". While he felt that the action requested by the R.C.M.P. in that instance was justified, "in view of the national and international implications" it was regrettable that the postal inspector did not deal with the matter "more intelligently". It was Mr. Boisvert's opinion that the postal inspector in Toronto should not have written a memo to Hamilton, and that the mail should not have been directed from Hamilton to Toronto and back to Hamilton. Mr. Boisvert assured the Minister that he was taking measures to avoid such incidents in the future.

24. As a result of this incident, on November 18, 1976, Mr. Boisvert met with the Deputy Director General (Operations) and the officer in charge of the Sources Branch concerning R.C.M.P. requests for Post Office co-operation and assistance in matters relating to the national security of Canada. It was decided at the meeting that any requests from the R.C.M.P. for special investigations of the mail in cases where it was considered "in the best interest of Canada and the public", would be funneled through the Ottawa offices of the Security and Investigation Services Branch. The decision as to whether co-operation should be extended by the Post Office would be made by Mr. Boisvert as the Director of Security and Investigation Services, or by the Chief of Investigations. If it were decided that co-operation was to be extended, the Regional Chief Inspector would be contacted and instructed accordingly. R.C.M.P. field units were not to seek assistance at the local levels, and any such requests were not to be accommodated.

25. In Mr. Boisvert's letter to the Regional Chief Inspector, he confirmed that "under no circumstances will the Canada Post Office permit mail to be illegally opened, delayed, tampered with or be removed from our premises". The R.C.M.P. report of this meeting is dated November 22, 1976, signed by Assistant Commissioner M.S. Sexsmith as Deputy Director General (Operations), and sent to all Divisions. Assistant Commissioner Sexsmith's guidelines, as sent out to the field correspond to the guidelines sent by Mr. Boisvert to the field.

26. From and after November 22, 1976, approval for all Cathedral operations was centralized at Headquarters, (Ex. B-20). At the same time area commanders were advised of the new policy which required that, instead of field units making arrangements with local post office people, all requests for Cathedral operations were to be sent to Headquarters for approval by either the Director General or the Deputy Director General (Operations). Assistant Commissioner Sexsmith testified that, while he had not authorized any Cathedral "C" operations since August of 1975, he had approved several Cathedral "A" and "B" operations.

27. Although Assistant Commissioner Sexsmith had not authorized any Cathedral "C" operation since August 1, 1975, he became aware, as a result of research undertaken in the R.C.M.P. in preparation for his appearance before us, that during 1976 a "local initiative" by a member or members of the Security Service had resulted in the opening of two letters in the OMURA case in Toronto. This case is dealt with in some detail in Part V, Chapter 4.

28. In addition, Assistant Commissioner Sexsmith testified that in July 1976 he was told of an operation in Ottawa by a member of the Security Service which was directed against foreign intelligence officers. Approval for the operation had been given in 1975. During the operation, on three or four occasions a letter posted was retrieved by members of the Security Service while it was in the course of the post. Assistant Commissioner Sexsmith gave instructions to cancel the operation, and it was stopped in July 1976.

29. Apart from the two incidents mentioned above, Assistant Commissioner Sexsmith believed, at least until the detailed review undertaken for the

purposes of the Commission, that the policies he introduced in August 1975, had been followed in the Security Service. However, it is apparent that two additional Cathedral "C" operations were approved at the divisional level during 1976 in direct violation of the formal policy of the Security Service.

30. In September 1977, the officer in charge of the Legal Branch of the R.C.M.P. was asked to consider the effect of the Post Office Act on mail check operations. He consulted with the legal adviser to the Post Office Department and in a memorandum (Ex. B-21) stated that it was illegal for anyone to open and examine mail with or without the co-operation of the postal authorities at any time after posting and before delivery. He also stated that he was not aware of any regulations or postal policy restrictions which would prevent the R.C.M.P., with the co-operation of the postal authorities, from viewing or photographing (not x-raying) any specific items of such *en route* mail. He cautioned, however, that care should be taken that any such mail not be detained.

31. As a result, on September 23, 1977, Headquarters sent a message to all area commanders (Ex. B-22), which quoted the text of the memorandum, and continued:

> ...It is emphasized that a Cathedral "B" operation must not go beyond examination of the outside of mail... Cathedral "A" and "B" requests will continue to require Director General or Deputy Director General (Operations) approval. As has been the practice in recent years Cathederal "C" requests will not be considered.

32. Assistant Commissioner Sexsmith, testifying before us in December 1977, said that the message set out the current policy and procedure of the R.C.M.P. Security Service.

33. After the question of mail check operations had become a matter of public discussion as a result of a television programme broadcast on November 8, 1977, Assistant Commissioner Sexsmith sent a directive, dated November 21, 1977, to area commanders, which he said resulted from the knowledge which he had recently acquired, that in "very few instances" after he began his term of office on August 1, 1975, Cathedral "C" operations had occurred without the approval of Headquarters. The message (Ex. B-23), states:

> It is therefore necessary to make clear that all Cathedral operations with the exception of the Cathedral "A" category, will not be entertained under any circumstances. As a result of discussions with postal authorities, it has been agreed that they will continue to co-operate on Cathedral "A" requests which are not illegal. There is one important stipulation to the effect that mail must not leave postal premises and must not leave the possession of postal authorities. Mail covers may be photographed or photocopied provided secure facilities are available on post office premises, but again under no circumstances is mail to be removed from postal premises nor is it to be delayed for any reason.
>
> This policy must not be abrogated for any reason whatsoever. Regardless of the rationalization, no deviation however slight, shall be tolerated. It will be the duty of every area commander to ensure that this policy is strictly adhered to.

> Please ensure that Cathedral "A" requests are fully supported with complete rationale when seeking authorization.

This directive was in its essentials the same as the message of September 23, 1977.

(b) *Criminal Investigation Branch*

34. A review of the use of mail check operations in criminal investigations by the R.C.M.P. was more difficult than the review of the use of such techniques by the Security Service because the C.I.B. did not have any centralized system of authorization or record keeping. It was apparent, however, that mail check operations became increasingly important to the C.I.B. in the late 1960s and 1970s because of increasing use of the mails for the importation and distribution of drugs.

35. Policy with respect to the subject was dealt with in successive issues of the R.C.M.P. Operations Manual. The earliest Manual page that could be located that dealt with this matter was dated June 15, 1972 (Ex. B-27).

> Section 41 of the Post Office Act protects mail in transit from seizure, except under the Customs Act. When you wish to search postal premises, consult with the senior local representative of the Post Office Department and arrange a postal inspection as postal officials are given additional powers under the Act.

Since February 1973 the Manual has contained more detailed instructions.

36. In December 1973 the Director of Criminal Investigations sent a memorandum (Ex. B-28), to the commanding officers of the various divisions concerning "Co-operation with the Post Office Department". After quoting what is now section 43 of the Post Office Act he said:

> The Postal Department does not wish to jeopardize the co-operation which presently exists between their investigators and our members, nor restrict our drug investigations in any way. However, when it is anticipated during an investigation that the Post Office co-operation will be brought out in court proceedings the following policy is to be adhered to:
>
> > Parcels or letters committed to the mail service will not be opened nor the contents interfered with, except during Customs examinations. To determine that a parcel originating in one area of Canada is the same parcel which is received and delivered at some other location in this country... (this was followed by a description of the technique).

37. At the time of the hearings before the Commission the instructions to the Drug Enforcement Branch were given by a bulletin (Ex. B-29), from the C.I.B. Directorate at Headquarters reminding members of the Force that in investigating illicit use of the mail system they were to "ensure that [they] are familiar with the Post Office Act and particularly s.43 and 46". At the time of the hearings before us in December 1977, a new memorandum of instructions was in the course of preparation.

C. EXTENT AND PREVALANCE OF THE PRACTICES

—

SECURITY SERVICE AND C.I.B.

(a) *Security Service*

38. A detailed review of the records of the Security Service was undertaken to determine the extent and prevalence of Cathedral operations during the period from November 1970 to the end of December 1977. A total of 94 mail check operations were identified of which 66 involved the actual opening of mail (Cathedral "C") and in two more cases opening was authorized but not carried out. Of these 66 cases, 21 occurred in the period of 1970 to 1973 in Quebec and were related to persons known or suspected to be involved in F.L.Q. terrorist activities. Another 11 related to persons known or suspected to be involved in international terrorism. Suspected espionage activities and foreign interference in Canadian political affairs accounted for 25 more cases, and there were nine miscellaneous targets.

39. The examination of the exterior of envelopes without photographing them (Cathedral "A") occurred in six cases, of which four related to suspected international terrorists, and two related to suspected or known espionage.

40. The examination and photographing of the exterior of envelopes (Cathedral "B") occurred in 19 cases and was authorized but not carried out in one other case. Of these 20 cases, 11 related to suspected international terrorists, and nine related to suspected or known espionage.

41. The Post Office Department also conducted several surveys at the Commission's request. In November 1977, the Post Office conducted a telephone survey across the four regions, Atlantic Region, Quebec, Ontario and Western Region. Subsequently, Post Office officials conducted interviews with 79 postal inspectors across the country. This series of interviews related to the relationship of the Post Office specifically with the Security Service of the R.C.M.P., rather than with the entire Force.

42. Of the Post Office surveys, the first survey, conducted over the telephone on November 9, 1977, was intended to ascertain what knowledge the regional Chief Inspectors had of the degree and number of requests which might have been made to the Post Office by the R.C.M.P. for either the opening of mail, or mail cover checks, for the period of November 1976 to November 1977. The results were as follows:

(a) Response from the Atlantic region indicated that although there were some local contacts prior to 1976, the two requests originating from the R.C.M.P. in the one-year period from November 1976 to November 1977 were both turned down by the Post Office.

(b) The Ontario region advised that it had received several requests through the Ottawa office during that year, and that there had been local contact prior to November 1976. According to the information provided by the Chief Inspector of the Ontario postal region, no mail was ever turned over

to the R.C.M.P., and no cover checks carried out, though mail covers may have been photocopied in the Ontario region Security and Investigation office.

(c) Quebec postal region office was aware of several requests since November 19, 1976, as well as some local contact prior to that time, but it maintained that no mail had ever been turned over to the R.C.M.P.

(d) As far as the Western region was concerned, some requests had been made for mail cover checks before November 19, 1976. No further requests were made after that date. Also, no mail was handed over to the R.C.M.P., or left the Post Office.

43. Post Office officials then conducted a more detailed interview survey of postal inspectors, past and present, from across the country. Selection of the postal inspectors was based on R.C.M.P. Security Service statistics which indicated where, according to their records, mail may have been opened in the course of Cathedral "C" Operations. At that time Security Service statistics pointed to 70 Cathedral "Cs", and therefore an effort was made to interview 79 postal inspectors. Forty of the inspectors interviewed indicated that they were never involved in any opening of the mail. Of the remaining 39 inspectors, 32 were current inspectors at the time of the interviews, and seven were former inspectors. Of the 32 current inspectors, two had given verbal statements to the Minister on November 16, 1977. One other refused to give a statement, another two were on sick leave at the time, and three others were not interviewed because they were not employed in the relevant area at the relevant time. One said orally that he had no involvement but refused to give a statement in writing, seven stated they were not involved because they were not present at the time and place suggested. The remaining group of 16 was not interviewed because information from the R.C.M.P. was that, although authorization to open mail had been granted, the procedures were not implemented; therefore no mail was opened in those instances. Of the seven former inspectors, two could not be located because their addresses were unknown and five refused to give statements.

(b) *Criminal Investigation Branch*

44. It was not possible to determine the extent and prevalence of mail check operations of the C.I.B. from centralized records, nor were the various types of check neatly classified by any code names such as Cathedral "A", "B", and "C". Because the interest of the C.I.B. arises particularly from the use of mails for the importation or distribution of drugs, the C.I.B. used the additional technique of "controlled delivery". Two instances, cited to us, in which this technique was employed, were (a) the receipt of advance information from foreign countries indicating that as many as 260 letters containing drugs would be arriving in the course of mail, and (b) Customs examination of packages disclosing the presence of drugs. In such circumstances members of the R.C.M.P. might participate in the delivery of mail to assist in the apprehension of the intended recipients after delivery is clearly established and before the drugs are put in circulation (Vol. 8, pp. 1119-20).

45. An attempt was made to have local divisions check for mail intercepts of all kinds. The results are summarized in Exhibit B-84 and in the evidence of Assistant Commissioner Venner (Vol. 18, pp. 2802-19). From this it will be seen that the vast majority of incidents related to enforcement of the laws concerning drugs. The difficulties occasioned by the definition of "letter", "first-class mail", "post letter" and "delivered" as discussed later in this chapter make the results questionable. Nevertheless, the following points are clear concerning the years 1970 to 1977:

(a) There were 954 mail intercept operations.

(b) Of these, 799 involved the opening of pieces of mail.

(c) Of the 799 cases, 100 involved mail within the dictionary definition of "letter", being "a written or typewritten communication on a piece of paper". The remainder (699) fell within the post office's broader definition of "post letters".

In addition, 592 pieces of mail were examined externally, and 258 pieces of mail were delivered under controlled circumstances.

46. These statistics provide a general indication of the extent and prevalence of mail openings and mail check operations on the criminal investigation side of the Force. They also show a great variance in different parts of the country in the interpretation and application of provisions of the Post Office and Customs Acts. It may be noted that there were no reported instances of C.I.B. mail interception in Quebec in search of either drugs or other substances. The explanation provided by "C" Division in Montreal for their statistics, which indicate that no mail was opened, rested on their position that anything other than "a simple envelope with obvious written communication inside is not first-class mail, regardless of the postage paid on it", and it was felt that it was not improper to open such other mail.

47. Assistant Commissioner T.S. Venner testifying before us on February 1, 1978, said that the postal customs authorities in Montreal were and are

> much more active in the opening of mail. . . than they are anywhere else in Canada. Our people simply found it necessary to get that involved. They rely on the postal customs people to alert them as to what they have found, and, in some cases, put the material back in the system for control and delivery and the openings are not done by our people.
>
> (Vol. 18, p. 2803.)

(Assistant Commissioner Venner subsequently informed us that he believes he said "unnecessary", not "necessary". We are satisfied that whatever he said, he clearly meant "unnecessary".) He explained also that another reason for non-activity by members of the drug section in Montreal in opening mail is that they "are not usually working on the kind of international cases which involve the smuggling of quantities of heroin by mail" but on importation cases which involve the use of couriers.

48. In contrast, in Southern Ontario, 389 pieces of mail were opened to determine whether drugs or other substances were contained in them. Of the 389 opened in Ontario, 252 were second or other class mail. It was not clear

what percentage of the remaining pieces of mail were first class. Furthermore, it was not clear how many pieces were opened by Customs and Postal officials, and the suggestion was made that none were opened by the R.C.M.P. but rather they were inspected or seen by the R.C.M.P. after having been opened by persons other than a member of the R.C.M.P. That, of course, is not an end of the legalism, for, if a source in the Post Office undoubtedly opens a letter, he commits an offence under section 58 of the Post Office Act; and a member of the R.C.M.P. who encourages him to do so is a party to the offence by virtue of section 21 of the Criminal Code. The offence depends on the opening being "unlawful" and that element of unlawfulness might be satisfied by the fact that the postal employee may have committed an offence under section 387(1)(c) of the Criminal Code ("Everyone commits mischief who wilfully... (a)... interferes with the lawful use, enjoyment or operation of property") or at least the tort of conversion. Vancouver was the other city which showed a large number of pieces of mail opened in the search for drugs: 406 pieces of mail were intercepted in search of drugs and five pieces of mail were intercepted in the search for other material.

49. In order to examine the extent and prevalence of mail intercept and mail opening practices by the R.C.M.P., it was necessary, in addition to the general statistics, to look at what might be involved in any single Cathedral or Mail Intercept Operation. One Cathedral Operation may involve numerous pieces of correspondence that are either checked on the cover or opened. The Commission heard evidence on behalf of both the Security Service and the Criminal Investigation Branch concerning specific examples of Mail Opening or Cathedral Operations. In the OMURA Case, presented by the Security Service, there were two instances of mail opening not authorized by Headquarters out of 50 items of mail examined.

50. On the criminal investigation side of the Force, eight cases were reviewed publicly and in each case some of the parcels were opened either while in the course of post, or after delivery. In most cases the openings were of international mail by Customs officials, with R.C.M.P. officers assisting or taking over for controlled delivery procedures.

D. LEGAL AND POLICY ISSUES — SECURITY SERVICE AND C.I.B.

Statutory provisions

51. The following are the relevant provisions of the Post Office Act.

(a) A definition of ownership of the mail is found in section 41:

> 41. Subject to the provisions of this Act and the regulations respecting undeliverable mail, mailable matter becomes the property of the person to whom it is addressed when it is deposited in a post office.

Thus an addressee has a property interest in mail once it is deposited in a post office. Consequently, any tampering with it is in some sense unlawful unless it is done by consent of the addressee or by statutory provision.

(b) A prohibition against "demand, seizure or detention" is found in section 43:

> 43. Notwithstanding anything in any other Act or law, nothing is liable to demand, seizure or detention while in the course of post, except as provided in this Act or the regulations.

This is the section which overrides search warrants under the Criminal Code or ministerial warrants under section 16 of the Official Secrets Act.

(c) Sections 58 and 59 create offences. Of these, section 58 is the more important for our purposes, as it makes it an indictable offence to delay or detain any article of mail unlawfully, or to open it or suffer it to be opened unlawfully:

> 58. Every person is guilty of an indictable offence who unlawfully opens or wilfully keeps, secretes, delays or detains, or procures, or suffers to be unlawfully opened, kept, secreted, or detained, any mail bag, post letters, or other article of mail, or any receptacle authorized by the Postmaster General for the deposit of mail, whether the same came into the possession of the offender by finding or otherwise.
>
> 59. Every person is guilty of an indictable offence who abandons, obstructs or wilfully delays the passing or progress of any mail or mail conveyance.

52. There are only two exceptions to section 43 in the Post Office Act. The first exception, found in section 7, allows the Postmaster General to detain mail, and in certain cases, forward it to a Board of Review that may open and examine it "with the consent of the person affected". The requirement that notice be given to the person affected renders this section inappropriate for criminal or security investigations.

53. The second exception is found in section 44 (formerly 46) which empowers Customs Officers to examine international mail, and provides in subsection 2:

> (2) A customs officer may open any mail, other than letters, submitted to him under this section, and may
>
> (a) cause letters to be opened in his presence by the addressee thereof or a person authorized by the addressee; or
>
> (b) at the option of the addressee, open letters himself with the written permission of the addressee thereof;
>
> and where the addressee of any letter cannot be found or where he refuses to open the letter, the customs officer shall return the letter to the Canada Post Office and it shall be dealt with as undeliverable mail in accordance with the regulations.

A member of the R.C.M.P. becomes part of this process by virtue of section 17(4) of the R.C.M.P. Act, which states as follows:

> (4) Every officer, and every member appointed by the Commissioner to be a peace officer, has, with respect to the revenue laws of Canada, all the rights, privileges and immunities of a customs and excise officer, including authority to make seizures of goods for infraction of revenue laws and to lay informations in proceedings brought for the recovery of penalties therefor.

Further, the Customs Act,[3] in section 2(1) defines officer as:

> ...["officer" means] a person employed in the administration or enforcement of this Act and includes any member of the Royal Canadian Mounted Police;

Effect of section 43 on section 16 of the Official Secrets Act

54. Section 16(2) of the Official Secrets Act provides that:

> (2) The Solicitor General of Canada may issue a warrant authorizing the interception or seizure of any communication if he is satisfied by evidence on oath that such interception or seizure is necessary for the prevention or detection of subversive activity directed against Canada or detrimental to the security of Canada or is necessary for the purpose of gathering foreign intelligence information essential to the security of Canada.

55. On the face of it, "any communication" would seem to include postal or written communication. As has already been recounted, Mr. Allmand signed a warrant in 1976 authorizing the interception of written communications subject to an opinion from the Department of Justice. The opinion, however, indicated that even though the word "communications" was seen by the Department of Justice as including letters, the wording of section 43 of the Post Office Act was so clear as to preclude section 16(2) of the Official Secrets Act from enabling the opening of letters in the course of post.

56. In Chapter 3 of this Part, where we discussed in detail the legal issues relating to Electronic Surveillance, we considered whether section 16(2) is, in our view, available at all in respect of letters. In section E of this chapter, and more fully in Part V, Chapter 4, we make recommendations as to the circumstances and conditions in which the opening of mail should be permitted in security matters.

International mail

57. It will be recalled that, pursuant to section 46(2) of the Post Office Act, a Customs Officer (which, pursuant to the Customs Act, includes any member of the R.C.M.P.) may open any mail *other than letters*. However, the Post Office Act does not contain a definition of "letter". It does contain, in section 2(1), a definition of "post letter":

> "post letter" means any letter deposited at a post office, whether such letter is addressed to a real or fictitious person, is unaddressed, and whether intended for transmission by post or not, from the time of deposit at a post office to the time of delivery and includes any packet prepaid or payable at letter rate of postage;

It will be observed that the definition appears to be intended to be broad in scope. In the absence of a statutory definition, the dictionaries tell us that a "letter" is a "written or printed message addressed to person(s), usually sent by post or messenger and fairly long" (Concise Oxford Dictionary); "a direct or personal written or printed message addressed to a person or organization"

[3] R.S.C. 1970, ch.C-40.

(Webster's New Collegiate Dictionary). There do not appear to be any Canadian judicial decisions interpreting "letter", but in the United States the word has been construed as meaning "a communication in writing from one person to another at a distance, and a written or printed message".[4]

58. The evidence before us has shown that at least in one major point of arrival for international mail there is a narrow interpretation of "letters" as that word is used in section 46(2) by Customs officials. In Montreal they feel free to open all international mail except "a simple envelope with obvious written communication inside", (Vol. 18, p. 2803). If this interpretation were used in all centres, there would be no impediment to the opening of any envelope or packet in "international mail" that appears to contain something other than a "written communication". However, the Montreal interpretation is not common, and therefore the Customs officials and R.C.M.P. in other centres are constrained not to open mail that would be opened in Montreal, although we do not have clear evidence as to the criteria used elsewhere.

59. The confusion becomes compounded when it is realized that, under the Post Office International First Class Mail Regulations,[5] "first class mail" is defined as including not only letters and postcards in handwriting or typewriting but also *any* item of mail that the sender chooses to prepay at first class rates. Thus parcels as much as one cubic foot in size might, pursuant to the size and weight limitations contained in those regulations, be "first class mail" if there is first class postage prepaid. We note this simply because so many news reports have spoken of the legal issue as being whether the R.C.M.P. or a postal employee may lawfully open international "first class mail". In fact, as we have seen, section 46(2) empowers customs officers to open *any* mail, of whatever class, without the addressee being present or having given his permission — except in the case of "letters". Consequently, while we have noted the international first class mail regulations, we do not believe that they are relevant to the legal problem.

Domestic mail

60. We turn now from international mail to domestic (solely within Canada) mail and all mail from abroad or addressed to a foreign destination while it is in the course of post in Canada. The prohibition contained in section 43 applies to all these kinds of mail: it is not subject to "demand, seizure or detention". Moreover, under section 58, it is an indictable offence to open any "article of mail" unlawfully or wilfully to "delay" or "detain" it. The "unlawfulness" of opening mail as such is found in a breach of the prohibition contained in section 43. We now apply those provisions to several possible domestic situations.

(a) Examining the exterior of an envelope (what the Security Service has called Cathedral 'A') might be unlawful if the length of time it is taken out of the mail stream results in its being "detained" or "delayed". Even if

[4] *Buckwald* v. *Buckwald*, 199 A. 795 at 799, 175 Md 103.
[5] S.O.R./71.336.

that were not so on the facts of most situations, it might be argued that a civil wrong is committed by interfering in the ownership of the article of mail, but this is doubtful. On balance, we do not believe that this investigative practice, if it does not involve removing the article from the mail stream for any significant length of time, can be said to be an activity "not authorized or provided for by law". This is particularly our view if the article of mail remains at all times in the control of a postal employee. Our view is the same as that of the Director of the Legal Services Branch of the Post Office, given in December 1977. Nevertheless, as will be seen, we consider that this technique involves such a degree of intrusion into the privacy of the persons involved that a higher level of approval of such an operation should be required than has been so in the past.

(b) The same remarks apply to photographing the exterior of an envelope (what the Security Service has called Cathedral 'B').

(c) If a postal employee hands an article of mail to a member of the R.C.M.P. so that he may open and examine its contents, both he and the R.C.M.P. member may be guilty as being accessories under section 58 of opening an article of mail unlawfully. The unlawfulness will lie in wilfully interfering with the lawful use, enjoyment or operation of property, which is mischief under section 387(1)(c) of the Criminal Code, or in the civil wrong of conversion, which involves even a temporary interference with another person's interest in property. Even if there is any doubt about that, the time taken to carry out the operation, especially if the opening is carried out off postal premises, may well constitute wilful delay or detention. Consequently, for one reason or another what the Security Service has called Cathedral 'C' would likely be an offence.

(d) Controlled deliveries: there are several techniques of controlled delivery which must be examined:

(i) The first situation involves the substitution of other innocuous substances for most of the drug found in any one item of mail, leaving only a small part of the original substance. The item of mail is then resealed and placed back in the system for delivery by postal officials. In this case it may be argued that the mail was not detained as long as this procedure was expeditious. Opinions written by legal officers of both the Department of Justice and the Post Office have so indicated. However, the point may also be made that the addressee's property has been tampered with, and that gives rise to the issues of mischief and conversion that have already been discussed, as well as theft.

(ii) The second situation involves the same type of substitution, but the delivery itself is by disguised members of the R.C.M.P. to the addressee's residence, rather than by postal officials. In this case, as in the first, if the procedure is effected expeditiously, it would not appear that section 58 concerning detention of mail is breached. The second point, however, still remains the same; there may have been such tampering as gives rise to issues of mischief, conversion and theft.

(iii) The third situation is exactly the same as the second, with the provision that the delivery to the addressee's residence is made by a disguised officer at a pre-arranged time under surveillance by R.C.M.P. members. This situation would probably involve the detention of mail, depending on the length of the delay involved in pre-arranging the delivery.

(iv) The fourth situation involves removal of an article of mail from the post office premises to an R.C.M.P. laboratory, its being opened there and its being subsequently resealed and returned to the post office for one of the previous three methods of controlled delivery. This clearly results in wilful detention and delay contrary to section 58.

(e) In an examination or photographing of envelopes, or opening an article of mail, before it is deposited in a "post office" (which includes a letter box), nothing is being done to an article in the course of post, and so the Post Office Act is inapplicable. A member of the R.C.M.P. could lawfully employ any of these techniques pursuant to section 10 of the Narcotic Control Act if he has a writ of assistance, the search is not of a dwelling-house, and he reasonably believes the article of mail contains a narcotic. If these conditions are not satisfied, any of these techniques might result in trespass, mischief, or conversion, depending upon the circumstances.

(f) The observations made in (e) apply to the examination or photographing of envelopes, or opening an article of mail, after it is delivered to a locked post office box, apartment box or rural mail box.

(g) In the case of letter bombs, if it is *known* that an article of mail contains an explosive, then the article of mail is considered "non-mailable matter" under sections 1 and 2 and Schedule I of the Prohibited Mail Regulations, and consequently, whether it is domestic mail (section 44 of the Act) or International mail (section 46(4) of the Act), it is to be disposed of by the Postmaster General's Department "in a manner that will not expose postal employees to danger" (section 4 of the Regulations). However, no assistance is provided by the Act or Regulations where there is mere reasonable belief that an article of mail contains a bomb, or only suspicion that it may do so. In such cases it appears that a postal employee or a member of the R.C.M.P. who opens an article of mail commits an offence under section 58, except when the mail is international and the article opened (by a Customs Officer, which includes R.C.M.P. members) is not a "letter".

61. Counsel for the R.C.M.P. suggested to us that the R.C.M.P.'s power to open mail might be available on the basis of the Crown prerogative, but in our view, even if there were some such prerogative power rooted in history, the Post Office Act, by prohibiting demand, seizure and detention in section 43 and thus making opening "unlawful" under section 58 if it involves demand, seizure or detention, has precluded any possibility of sustaining an argument that opening is lawful by virtue of the exercise of a prerogative.

E. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

62. In Part V, Chapter 4, we conclude that the need exists to permit the security intelligence agency lawfully to open envelopes and read messages. However, the use of this technique should be strictly and carefully controlled in individual cases, and the subject of regular and prudent study by the independent review body which we shall recommend be established. The power to use these techniques should be limited to the investigation of espionage, foreign interference and serious political violence.

63. As for the criminal investigation side of the Force, we conclude in Part X, Chapter 5 that peace officers should have the power to examine or photograph an envelope or to open mail only in narcotic and drug cases. This power should be limited to examination and testing of any substance found in the mail. Unless a narcotic or restricted drug is found in the mail reading an accompanying message should be made an offence. Peace officers exercising this power should require a judicial authorization subject to the same safeguards as are now found in section 178 of the Criminal Code governing the use of electronic surveillance.

CHAPTER 5

ACCESS TO AND USE OF CONFIDENTIAL INFORMATION HELD BY THE FEDERAL GOVERNMENT — CRIMINAL INVESTIGATIONS

A. ORIGIN, NATURE AND PURPOSES OF PRACTICES

1. The various departments and agencies of the federal government are a storehouse of personal information about Canadian citizens and others who are required under various statutes to provide that information to the government. This is particularly so with respect to the income tax records of the Department of National Revenue and the employment records of the Canada Employment and Immigration Commission. Access to the government's store of information has a strong attraction for the R.C.M.P., both for their own use and to assist other police forces, at home as well as abroad. In investigating offences, keeping the peace or simply assisting members of the public, the R.C.M.P. need all available sources of information and obviously, the more they have available, the better able they will be to resolve a given problem.

2. On the other hand the government, for several reasons, has felt it advisable to restrict access to personal information provided to it by individuals. In addition to the general reluctance to have the privacy of individuals invaded unnecessarily, the government recognizes the need for confidentiality of tax records if it hopes to operate a tax system which, although compulsory in law, is in reality based on voluntary compliance. The government has also believed that, to obtain public co-operation in a universal social insurance scheme (including manpower and unemployment insurance programmes), it has to provide an assurance that the information received by it will not be disseminated for other purposes. Consequently, many statutes which compel production of such information include restrictions on access to it. The R.C.M.P., in the pursuit of its duties, has breached those provisions either with specific approval from Headquarters, as a Force policy, or with the tacit approval of senior officers. As will be seen in this chapter, this practice of law-breaking became institutionalized within the R.C.M.P.

3. The Criminal Investigation side of the R.C.M.P. has sought access to five distinct sets of government records: the income tax records of the Department of National Revenue, the employment records of the Canada Employment and Immigration Commission (formerly the Unemployment Insurance Commission), the family allowance and old age security records of the Department of

National Health and Welfare, the Industrial Research and Development Incentives Act financial grant records of the Department of Industry, Trade and Commerce and finally the records compiled by the Foreign Investment Review Agency pursuant to the provisions of the Foreign Investment Review Act. We shall now examine those five cases in detail.

B. DEPARTMENT OF NATIONAL REVENUE

Policy and implementation

4. The relationship between the Criminal Investigations (C.I.B.) side of the R.C.M.P. and the Department of National Revenue (D.N.R.) has varied over the years. At present that relationship covers two distinct areas: first, the routine enforcement of the Income Tax Act which includes the location and prosecution of delinquent taxpayers, and second the organized crime Tax Programme (Vol. 47, pp. 7582-3). That programme, which we shall describe in detail later, is an agreement between the R.C.M.P. and the D.N.R. to co-operate in enforcing the provisions of the Income Tax Act against persons described as being involved in "organized crime". We heard considerable evidence as to how different people working on the programme defined "organized crime", but since for the purposes of examining the legality of the actions of the people involved the definition of "organized crime" is not pivotal, we will not examine it other than to quote one definition used by the R.C.M.P.: "two or more persons concerting together on a continuing basis to participate in illegal activities either directly or indirectly for gain" (Ex. G-1, Tab 35).

5. The activities of the R.C.M.P. relating to the routine enforcement of the Income Tax Act include the locating of delinquent taxpayers, laying of informations and complaints, serving summonses and executing warrants of commitment and of arrest, and obtaining search warrants (Vol. 47, pp. 7583-7; Ex. G-1, Tab 3; Ex. G-2 for identification, Tabs 1 and 2). The primary responsibility for enforcement of the Income Tax Act lies with the D.N.R. and the responsibility of the R.C.M.P. in this regard is secondary (Vol. 47, p. 7594). This area of relationship is of long-standing duration and in itself has not given rise to any misconduct which we have been able to uncover.

6. Most of the activities which have been the subject of our concern arose out of what came to be known as the Tax Programme. Prior to 1972 the R.C.M.P. passed information to the D.N.R., through a strictly informal arrangement, about criminals being investigated by the R.C.M.P. (Vol. 47, p. 7597). During the 1960s a number of factors motivated the R.C.M.P. to push for co-operation by the D.N.R. to fight organized crime. Those factors were: the collapse of certain financial institutions and the involvement of organized crime in associated bankruptcy frauds, a subject which was raised in Parliament and at a 1967 Federal-Provincial Conference; the 1964 Royal Commission on Banking, which mentioned problems in the securities industry; the success of a U.S. task force approach in this field; and the fact that some attorneys general at the 1965 Conference of attorneys general had felt that there should be some co-operation between departments to pursue the income of organized crime

figures (Vol. 47, pp. 7621-27, 7633-34; Vol. 62, pp. 9988-89; Ex. G-1, Tab 12; Ex. G-11, Tab 8; Ex. G-2 for identification, Tab 3).

7. Motivated by these factors, the R.C.M.P. initiated discussions with the D.N.R. with a view to working out arrangements not simply to transmit information to the D.N.R. but also to receive it. One of their reasons for wanting such an exchange was to be able to advise their sources of information that information supplied to the D.N.R. had been put to use. The R.C.M.P. felt that otherwise the sources of information might dry up (Vol. 47, pp. 7667-8).

8. To pursue the objective of closer co-operation, the R.C.M.P. arranged a meeting on November 1, 1967, with D.N.R. officials. According to a record of the meeting the D.N.R. officials present advised the R.C.M.P. that there would have to be a clear understanding in the D.N.R. that the department's involvement was not intended specifically to produce revenue from delinquent taxes but rather to assist in attacking organized crime. The records also show that the D.N.R. officials indicated that the Department did not have the manpower to help the R.C.M.P., but they spoke of the desirability of there being a "two-way exchange", since the then current interpretation of the Income Tax Act "allowed the release of certain information to the police under proper circumstances" (Vol. 62, p. 9988 and Ex. G-1, Tab 11).

9. The next recorded step in the development of this aspect of the relationship is a letter of January 31, 1969, from the Deputy Commissioner (Criminal Ops.) of the R.C.M.P. to the Deputy Minister of National Revenue (Taxation) requesting a meeting to discuss matters which might be of "mutual interest". The letter stated that the purpose of any co-operation would be to combat organized crime, the D.N.R. to assist "through active participation in such investigations". The letter added that the "exchange of information between them" should be a two-way effort (Ex. G-1, Tab 12). Following that letter, a meeting was held on February 18, 1969, between the Deputy Minister of National Revenue (Taxation), the official in charge of special investigations for the D.N.R., Deputy Commissioner Kelly and Assistant Commissioner Carrière, to discuss joint action to combat organized crime. A record of that meeting shows that:

> Kelly stated that this Force would be willing to liaise with members of [D.N.R.] to ensure a two-way exchange of information and where necessary, to treat any information received as strictly confidential. He added that the Force and himself were well aware in view of the content of Section 133 of the Income Tax Act that such a request could not be acceded to as this was not a matter of policy but a matter of law.
>
> (Vol. 47, pp. 7638-42; Ex. G-2 for identification, Tab 4.)

10. Another meeting was held between officials of the D.N.R. and members of the R.C.M.P. on April 23, 1969. The D.N.R. officials advised that Department policy with respect to dissemination of information from their files to the R.C.M.P. was limited to cases where the provisions of section 133(3) of the Income Tax Act applied. Both parties to the meeting admitted that, in spite of the official D.N.R. policy, there were "sometimes *sub rosa* arrangements made

at the Regional Level with respect to specific instances" (Ex. G-1, Tab 13). Prior to 1972 the official policy of both the D.N.R. and the R.C.M.P. was that all requests to the D.N.R. from the R.C.M.P. for assistance were to be directed to R.C.M.P. Headquarters in Ottawa (Vol. 62, pp. 9984-5; Ex. G-2 for identification, Tab 2; Ex. G-1, Tab 14).

11. In his testimony before us, the senior D.N.R. official present at that April 23, 1969 meeting told us that he did not consider that the words in the minutes of the meeting referring to "*sub rosa* arrangements" implied any deviation from official Department policy. He said that he interpreted those words to mean that there would have to be some exchange of information at the district level to determine whether the information was of any value (Vol. 62, pp. 10001-2). He also told us that it was his view at the time of the meeting, that the D.N.R. could furnish information to the R.C.M.P. where the Force would, in some way, assist the Department in collecting tax because that would be an enforcement of the Income Tax Act (Vol. 62, p. 9998). It is clear from the evidence before us that the official position of the D.N.R. at that time was that information could only be communicated to another agency if to do so would assist the Department in administering or enforcing the Income Tax Act (Vol. 47, p. 7651; Ex. G-1, Tab 14).

12. We have noted that on September 15, 1969, the officer in charge of the R.C.M.P. Legal Branch gave a legal opinion to the assistant officer in charge of the C.I.B. which stated that, before information could legally be given to the R.C.M.P. by the D.N.R. under section 133, "there must be a tax interest" (Ex. G-1, Tab 15).

13. Another high level meeting was held on October 29, 1969, between the Deputy Minister and officials of the D.N.R., and R.C.M.P. officers, to discuss a draft memorandum which had been prepared by the two agencies on the subject of "Co-operation relative to the investigation of organized crime". At that meeting the Deputy Minister insisted that there had to be a tax interest before any tax information could be released by an authorized person. The record of the meeting shows that the R.C.M.P. representatives present agreed with that interpretation and agreed to the deletion from the draft memorandum of a statement to the contrary which said, in referring to section 133(7)(a) of the Income Tax Act:

> These words could also be construed to mean that an authorized person could release the required information as part of his day-to-day job, and that no particular tax interest is necessary.

The Deputy Minister also advised the R.C.M.P., at that meeting, that direction would have to be sought from the government for the change in policy by the D.N.R. which would result from this new area of co-operation. He suggested that the R.C.M.P. prepare a draft memorandum to Cabinet for the signature of the Solicitor General (Vol. 47, pp. 7704-5; Ex. G-2 for identification, Tab 5).

14. At some point, probably in 1969, the Commissioner of the R.C.M.P. asked the Honourable G.J. McIlraith, the Solicitor General, to do something to enable the R.C.M.P. to obtain direct access to income tax returns for the

purpose of dealing with the subject of organized crime. In a letter dated January 21, 1970 to Mr. McIlraith, Commissioner Higgitt discussed obtaining access to tax data to attack organized crime from the revenue viewpoint. Mr. McIlraith testified that during that same period he had discussions with Commissioner Higgitt about the R.C.M.P.'s desire to get information from the D.N.R. to assist in the investigation of certain criminals in the organized crime field (Vol. 120, pp. 18707-9).

15. On March 20, 1970, the R.C.M.P. forwarded to Mr. McIlraith a copy of a draft memorandum to Cabinet which had been prepared by the D.N.R. and the R.C.M.P. (Vol. 47, p. 7705; Ex. G-2 for identification, Tabs 7 and 8). Mr. McIlraith told us that he was supportive of the R.C.M.P. obtaining clarification of what they were entitled to get from the D.N.R. He also told us that, from the time he was first approached with a request to do something to obtain direct access by the R.C.M.P. to income tax returns until he left the Solicitor General's portfolio on December 22, 1970, he refused to do anything about that aspect (Vol. 118, pp. 18472-4; Vol. 120, pp. 18707, 18734).

16. Following the receipt by Mr. McIlraith of the draft memorandum to Cabinet, which was forwarded to him on March 20, 1970, Commissioner Higgitt noted in his diary on April 23, 1970:

> Solicitor General asked re cooperative action by Income Tax Branch and R.C.M.P. Solicitor General said he would suggest to the Minister of National Revenue that the Act gave sufficient leeway.
>
> (Vol. 120, p. 18718; Ex. M-75.)

Several months later Commissioner Higgitt recorded in his diary entry of September 8, 1970 that he had had a meeting with Mr. McIlraith and he noted the following:

> Jogged Solicitor General's memory re income tax cooperation. He said he had spoken to the Minister (Mr. Côté) last week. He said his departmental people thought there ought to be a Cabinet paper. He, Côté, did not agree and would like the Solicitor General to clarify the matter before him, etc. This is to be done as soon as convenient.
>
> (Vol. 120, pp. 18722, 18733-34, Ex. M-76.)

On December 22, 1970, the Honourable Jean-Pierre Goyer succeeded Mr. McIlraith as Solicitor General. Sixteen months later, a joint memorandum to Cabinet dated April 27, 1972, signed by Mr. Goyer and the Minister of National Revenue, sought approval for the D.N.R., with the assistance of the R.C.M.P., to

> . . . conduct a continuing programme of tax investigations into the affairs of members of Organized Crime with a view to their prosecution under the Income Tax Act on the clear understanding that the restrictions set forth in section 241 of the Income Tax Act apply to members of the Force engaged in this enterprise and that they will be instructed not to communicate or knowingly allow to be communicated to any person other than to those persons designated by the Minister of National Revenue any information obtained by or on behalf of the Minister of National Revenue for the purposes of that Act.

The memorandum also provided: "No public announcement is contemplated" (Vol. 123, p. 19202; Ex. G-2c, Tab 7). The Cabinet granted approval for this programme, which was known as the Tax Programme, on May 25, 1972. Mr. Goyer testified before us that the objective of this contemplated programme was to combat organized crime while administering the Income Tax Act (Vol. 123, p. 19202).

17. Also on April 27, 1972, a Memorandum of Understanding between the Department of National Revenue (Taxation) and the Department of the Solicitor General was prepared and signed by the Deputy Ministers of the two Departments. This memorandum was subject to the approval by Cabinet of the proposal contained in the memorandum to Cabinet. In this Memorandum of Understanding, the method of putting into operation the proposal contained in the memorandum to Cabinet was made more specific. It provided as follows:

1. The Minister of National Revenue, pursuant to the provisions of subsection (4) of Section 241 of the Income Tax Act, hereby designates the members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police as authorized persons for the purpose of assisting him and his officials in carrying out investigations for such purposes as the Minister of National Revenue may designate related to the administration or enforcement of the Income Tax Act.
2. The Royal Canadian Mounted Police acknowledges that the members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police will conduct for the purposes of the Income Tax Act, such investigations of such persons as the Minister of National Revenue may from time to time request, except when the Solicitor General is of the opinion that having regard to the current tasks of the Royal Canadian Mounted Police and the availability of manpower, it is not practical for such investigations to be conducted.
3. The Minister of National Revenue will furnish the Directorate of Criminal Investigations of the Royal Canadian Mounted Police with such information or material in his possession which in the Minister's opinion will facilitate the conduct of any investigation which the Directorate of Criminal Investigations of the Royal Canadian Mounted Police is carrying out on behalf of the Minister.
4. The Royal Canadian Mounted Police acknowledges that all information obtained for the purposes of the Income Tax Act by the members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police in the conduct of investigations referred to in clause 2 hereof are subject to the restrictions set forth in Section 241 and that in particular, no member of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police will knowingly communicate or knowingly allow to be communicated to any person other than those persons designated by the Minister of National Revenue any information obtained by or on behalf of the Minister of National Revenue for the purposes of this Act.
5. The Solicitor General of Canada agrees to provide the Minister with the names of individuals whom the Directorate of Criminal Investigations of the Royal Candian Mounted Police suspects of being involved in organized crime and in evading or understating the amount of their income,

together with all intelligence information available to it on these individuals.

6. The Minister acknowledges that all information which he receives from the Solicitor General of Canada either prior to or as a result of investigations which have been carried on by members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police as authorized persons will be treated as confidential information and will not, without the express authority of the Royal Canadian Mounted Police, be disclosed to persons other then [sic] designated individuals who are members of the Special Investigations Division of the Department of National Revenue and their superior officers.

7. The Minister agrees that if he should conclude that any investigation which is being conducted by members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police pursuant to the provisions of clause 2 hereof is not likely to be fruitful and is being discontinued by his officials, he will immediately so advise the Directorate of Criminal Investigations of the Royal Canadian Mounted Police.

8. Members of the Directorate of Criminal Investigations of the Royal Canadian Mounted Police will assist National Revenue, Taxation to develop evidentiary standards to establish offences on the basis of testimony relative to cash transactions where documentation is limited or non-existent and will, in circumstances considered appropriate by both National Revenue, Taxation and the Royal Canadian Mounted Police, allow its criminal intelligence investigators to give evidence in court on their knowledge of financial transactions entered into and business procedures and techniques used by members of organized crime prosecuted by National Revenue, Taxation.

9. This agreement will take effect upon the approval by Cabinet of the recommendations contained in a memorandum to Cabinet by the Minister of National Revenue and concurred in by the Solicitor General dated April 27, 1972.

18. The Department of Justice assisted with the content and the drafting of the Memorandum of Understanding and gave an opinion that the agreement was legal. The Attorney General of Canada approved of the memorandum to Cabinet when it was drafted (Vol. 62, pp. 10011-16; Vol. C12, p. 1327).

19. According to the testimony before us of Inspector R.D. Crerar, the officer in charge of the R.C.M.P. Commercial Crime Branch, the kind of exchange of information envisaged by the Memorandum of Understanding is not different from that which was discussed at the meeting of April 23, 1969, i.e. it was limited to cases where the provisions of section 133(3) of the Income Tax Act applied (Vol. 47, pp. 7646-47).

20. It will be noted that the Memorandum of Understanding designated the members of the Directorate of Criminal Investigations as "authorized persons". Testimony before us disclosed that the Directorate of Criminal Investigations included the Commercial Crime Branch (C.C.B.), the National Crime Intelligence Branch (N.C.I.B.), the Contract Policing Branch, the Native Policing Branch, the Customs and Excise Branch, the Federal Policing Branch, the Drug Enforcement Branch and the Special "I" Branch. However, com-

munications from R.C.M.P. Headquarters to the divisions limited the application of the programme to the Commercial Crime Branch and the National Crime Intelligence Branch. The evidence also disclosed that within the R.C.M.P., the primary responsibility for carrying out the Tax Programme was assigned to the C.C.B. and the N.C.I.B., although there were times when other members were involved (Vol. 48, pp. 7741-45; Vol. C12, p. 1432).

21. We were told that it was the understanding of the D.N.R. that certain R.C.M.P. members within the Directorate of Criminal Investigations would be assigned to the Tax Programme and that they would be the "designated" persons. The R.C.M.P. did assign certain members to the programme (Vol. 62, p. 10019; Vol. 48, pp. 7753-55, Ex. G-1, Tab 17). The D.N.R. were assured by the R.C.M.P. that the Force would not disseminate taxation data outside the Force, and would only disseminate it within the Force on a strict 'need to know' basis. We heard evidence, which we shall discuss later in this chapter, that tax information was given to members of the R.C.M.P. who were not on the Tax Programme provided they had a 'need to know' (Ex. G-1, Tab 17, Vol. 48, pp. 7758-60). The current arrangement is that all R.C.M.P. members designated under the Tax Programme must be designated in writing by the Director of Criminal Investigations (Vol. 48, pp. 7830-39; Ex. G-1, Tab 23).

22. There was considerable evidence as to who were included in the definition of "organized crime" but, as we mentioned earlier, because we do not consider that a definition of that phrase affects the legal issues involved, we do not propose to summarize the evidence nor to come to any conclusion about it. It is clear that the D.N.R. did not particularly concern itself about a definition of "organized crime". An official of the D.N.R. involved in the Tax Programme testified that the Department always understood that the people being investigated under the programme were those involved in criminal activities and that the term "organized crime" was a more common phrase used to describe them (Vol. 62, pp. 10030-31; Ex. G-12, Tab 11B). As Mr. Justice Laycraft observed in 1978 the working definition of "organized crime" used by the R.C.M.P. is so wide as to include any two persons committing a second offence, and even "any person making his living from crime".[1]

23. Regardless of who is included in the definition of "organized crime", there does not appear to have been any difficulty or disagreement as to who ought to be the subjects or "targets" of the programme. Initially, the targets of the programme were provided by R.C.M.P. Headquarters. Subsequently, targets were selected at the local district level by agreement between the D.N.R. district official and the R.C.M.P. Unit or Section Commander. The R.C.M.P. Unit advised R.C.M.P. Headquarters of each such selected target, and on no occasion did Headquarters veto such a selection. The evidence disclosed that both the R.C.M.P. and the D.N.R. could suggest names of potential targets for consideration (Vol. 62, p. 10135; Vol. 62, p. 10058; Ex. G-11, Tab K; Vol. C48, p. 7767-72, and Ex. G-2, Tab 11).

---

[1] *Report of a Public Inquiry into Royal American Shows Inc. and its Activities in Alberta*, June 1978, at p. C-42.

24. The memorandum to Cabinet seeking approval for the Tax Programme indicated that no public announcement of the programme was contemplated, but there is nothing in the Memorandum of Understanding nor in the Cabinet decision that prohibits publication of the agreement. There was, however, an agreement between the Department of National Revenue and the Solicitor General's Department that the Memorandum of Understanding would not be published. Later, some pressure developed within the government to disclose publicly the existence of the Tax Programme. By letter dated March 11, 1975, the Honourable Ronald Basford, the Minister of National Revenue, wrote to the Solicitor General, the Honourable Warren Allmand, advising that it was his intention to make a public announcement regarding the programme. It appears that Mr. Allmand sought the advice of Commissioner Nadon on the matter, because a letter dated April 7, 1975, from Commissioner Nadon to Mr. Allmand, set out the arguments on both sides with respect to publication. That letter discloses that the main reason why, according to the R.C.M.P., the agreement should not be made public was that pressure groups would seek an amendment to the Income Tax Act which would make the Act more restrictive. Commissioner Nadon told us that, on balance, he had favoured publication of the agreement.

25. Mr. Allmand concluded that it was necessary to make a public announcement and, by letter dated May 10, 1976, he wrote to the Honourable Bud Cullen, the Minister of National Revenue, stating that it was imperative that some form of public announcement be made by Mr. Cullen's office. Mr. Cullen replied, by letter dated June 9, 1976, agreeing that there ought to be an announcement but added that there were some problems to be considered. He told Mr. Allmand that Cabinet authority for the agreement had been obtained on the assurance that no public announcement would be made and therefore express authority would have to be sought from Cabinet for a public announcement. He suggested that Mr. Allmand take the initiative in seeking such Cabinet approval and that he would support Mr. Allmand's position.

26. It is clear from the evidence that the R.C.M.P. and the D.N.R. had different reasons for wanting to keep the agreement secret. The R.C.M.P. wanted to keep it secret in order to combat organized crime. However, as time passed the targets of the programme became aware that they were being investigated by the R.C.M.P. through the reporting of cases coming before the courts in which the R.C.M.P. had acted as witnesses. As more targets became aware of the investigations there was less reason for the R.C.M.P. to maintain the confidentiality of the agreement. The reason the D.N.R. wished to keep the agreement secret was their concern that publication of it would damage the credibility of their assertion of the confidentiality of tax information.

27. Publication of the agreement eventually took place in the Fall of 1977, when its existence was made public as a result of the Inquiry of Mr. Justice Laycraft in Alberta.[2] Commissionner Nadon testified at the Laycraft Inquiry without the benefit of a review of the R.C.M.P. documentation with respect to possible publication of the agreement. He testified at that Inquiry that from

---

[2] *Ibid.*

the outset, and during the course of the agreement, the R.C.M.P. had endeavoured to have it published, whereas the evidence before us disclosed that at least on one occasion the R.C.M.P. were satisfied that publication would not be desirable.

28. On March 3, 1977, Commissioner Nadon met with the Attorney General of Alberta and at the meeting admitted that there was an agreement with the D.N.R., but he advised the Attorney General that its contents were confidential. Mr. Nadon refused to let the Attorney General see a copy of the agreement unless the D.N.R. first agreed to such disclosure. He advised the Attorney General that when the agreement was first entered into the R.C.M.P. had been in favour of it being published but that the D.N.R. had been opposed. Mr. Nadon told us that he considered that the agreement between the two departments not to publish superseded his responsibility in his relationship with the Provincial Attorney General because any disclosure by the R.C.M.P. would not only jeopardize other arrangements they had with the D.N.R. but also might preclude further information from being provided to the Force. (We discuss the relationship between the R.C.M.P. and provincial attorneys general in Part X, Chapter 4.)

Extent and prevalence

29. At our request, a memorandum dated December 20, 1977, was sent from R.C.M.P. Headquarters to the commanding officers of all R.C.M.P. divisions asking, *inter alia*, for the following information:

> Between 1969 and 1972, did R.C.M.P. Investigators obtain information from Income Tax files in contravention of Section 241 of the Income Tax Act? If so, under what circumstances, how many times etc.?
>
> *Subsequent to the 1972 Agreement*
>
> Were there any incidents when information received as per the Agreement was used for purposes other than enforcement of the Income Tax Act? e.g. disclosed to other R.C.M.P. sections which did not have lawful access such as — Security Service, Criminal Investigative Sections. If so, how many times, under what circumstances?

30. For the period from 1969 to 1972, the replies to that request for information did not disclose any specific cases of dissemination of information in contravention of the Income Tax Act. The reasons given in those replies are either that no such information was provided to the R.C.M.P. or that no records are available for that period to enable a reply to be given. The evidence discloses that there was, however, a recollection that the D.N.R. sometimes supplied biographical information to the Force (Ex. G2C, Tabs 12-27 inclusive, Vol. 48, pp. 7861-7910).

31. The replies, which were filed as exhibits with us, disclose that, for the period following the 1972 Memorandum of Understanding to the respective dates of reply from the divisions, there were numerous instances in which information was sought by R.C.M.P. members assigned to the Tax Programme and passed on by them to other branches of the R.C.M.P. and to other police forces, when such information was not being used for the purpose of enforce-

ment of the Income Tax Act. The evidence shows that in most of those cases the information was of a biographical nature but that in some cases it included financial information (Ex. G2C, Tabs 12-27; Vol. 48, pp. 7861-7910; Vol. 50, pp. 8016-43; Vol. 51, pp. 8260, 8270, 8317; Vol. 63, pp. 10320-32). The evidence also discloses that in many instances the D.N.R. officials involved were aware that the information they were passing to the R.C.M.P. members was not for the purposes of enforcement of the Income Tax Act (Ex. G-11, Tabs 1-28).

32. We were also told in testimony that there have been instances where the R.C.M.P. members involved in the Tax Programme have come across evidence of serious criminal offences and have felt that they were not able to proceed to prosecution with respect to those offences because they were not entitled to use the information for that purpose (Vol. 48, pp. 7850-6; Vol. 49, pp. 7945-6).

Legal issues

33. The Income Tax Act,[3] section 241, provides for the confidentiality of information given by a taxpayer to the Department of National Revenue. It also sets forth exceptions. It also makes it an offence to contravene the section. The relevant parts of the section are as follows:

> 241. (1) Except as authorized by this section, no official or authorized person shall
>
> (a) knowingly communicate or knowingly allow to be communicated to any person any information obtained by or on behalf of the Minister for the purposes of this Act, or
>
> (b) knowingly allow any person to inspect or to have access to any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act.
>
> (2) Notwithstanding any other Act or law, no official or authorized person shall be required, in connection with any legal proceedings,
>
> (a) to give evidence relating to any information obtained by or on behalf of the Minister for the purposes of this Act, or
>
> (b) to produce any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act.
>
> (3) Subsections (1) and (2) do not apply in respect of criminal proceedings, either by indictment or on summary conviction, under an Act of the Parliament of Canada, or in respect of proceedings relating to the administration or enforcement of this Act.
>
> (4) An official or authorized person may,
>
> (a) in the course of his duties in connection with the administration or enforcement of this Act,
>
> (i) communicate or allow to be communicated to an official or authorized person information obtained by or on behalf of the Minister for the purposes of this Act, and

[3] R.S.C. 1970, ch.I-5, as amended by S.C. 1978-79, ch.5.

(ii) allow an official or authorized person to inspect or to have access to any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act;

(b) under prescribed conditions, communicate or allow to be communicated information obtained under this Act, or allow inspection of or access to any written statement furnished under this Act to the government of any province in respect of which information and written statements obtained by the government of the province, for the purpose of a law of the province that imposes a tax similar to the tax imposed under this Act, is communicated or furnished on a reciprocal basis to the Minister;

(c) communicate or allow to be communicated information obtained under this Act, or allow inspection of or access to any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act, to or by any person otherwise legally entitled thereto; or

(d) communicate or allow to be communicated to a taxpayer, such information obtained under this Act regarding the income of his spouse or of any other person as is necessary for the purposes of an assessment or reassessment of tax, interest, penalty or other amount payable by the taxpayer or of the determination of any refund to which he is entitled for the year.

(a) *The general rule stated in section 241 of the Income Tax Act*

34. The section attempts to protect from unauthorized disclosure, a term which is discussed below, "any information obtained by or on behalf of the Minister for the purposes of this Act". It further restricts inspection of or access to "any book, record, writing, return or other document obtained by or on behalf of the Minister for the purposes of this Act."

(b) *The exceptions*

35. There are a number of exceptions to the general rule prohibiting disclosure. The rule does not apply in respect of criminal proceedings, either by indictment or on summary conviction, under an Act of the Parliament of Canada, or in respect of proceedings relating to the administration or enforcement of the Income Tax Act. Furthermore, an "official" or "authorized person" may:

(i) in the course of his duties in connection with the administration or enforcement of the Act, communicate or allow to be communicated to an official or authorized person tax information and allow an official or authorized person to inspect documents obtained for the purposes of the Act;

(ii) communicate information or allow inspection of documents to or by the government of any province for the purpose of administering a tax law of the province;

(iii) communicate information or allow inspection of documents to any person "otherwise legally entitled thereto";

(iv) communicate information to a taxpayer regarding the income of his spouse or of any other person in order to permit an assessment or reassessment of tax, interest, penalty, etc.

In addition, the Minister may permit a copy of a document containing tax information to be given to the person from whom such document was obtained, or to that person's legal representative or agent.

36. Who is an "official or authorized person" for the purposes of section 241 of the Income Tax Act? Section 241(10)(a) defines "official" as

> . . . any person employed in or occupying a position of responsibility in the service of Her Majesty, or any person formerly so employed or formerly occupying a position therein;

Subsection (b) of section 241(10) defines "authorized person" as

> . . . any person engaged or employed, or formerly engaged or employed, by or on behalf of Her Majesty to assist in carrying out the purposes and provisions of this Act;

37. The major difference between "official" and "authorized person" is that the section does not specify that the job or function of an "official" necessarily requires that it be "to assist in carrying out the purposes and provisions of this Act." It thus appears that an R.C.M.P. officer could fall within the definition of "official" as being "employed in or occupying a position of responsibility in the service of Her Majesty". This was the view of Mr. Justice Laycraft, in the Alberta inquiry.[4] If this is the case, then an R.C.M.P. officer does not need to be designated by anyone as an authorized person, and the prohibitions and sanctions of section 241 apply automatically as long as he is dealing with what has been termed above, for the sake of brevity, as tax information, and as long as this information has been "obtained by or on behalf of the Minister for the purposes of this Act."

38. On the other hand, an R.C.M.P. officer may become an "authorized person" if he is either seconded to the Department of National Revenue, or hired by the Department to perform work in connection with the Act or in some way "engaged. . . to assist in carrying out the purposes and provisions" of the Income Tax Act. Then he automatically becomes an "authorized person" and does not need to be so designated by anyone. The question whether someone is an "official" or "authorized person" thus becomes a question of fact.

39. What restrictions apply to the dissemination of biographical data provided to the Department of National Revenue by a taxpayer? Not only does section 241 of the Income Tax Act protect "any information obtained" as long as it is obtained for "the purposes of" the Act; it restricts access to any "book, record, writing, return or other document obtained" . . ."for the purpose of this Act."

---

[4] *Report of a Public Inquiry into Royal American Shows Inc. and its Activities in Alberta*, June 1978, pp. C-42-47.

40. One of the qualifying phrases is "for the purposes of this Act". The question then arises whether biographical information is information obtained for the purposes of the Act. Biographical information, as distinguished from financial information, would include the taxpayer's name, address, telephone number, employer's name, wife's and children's names, previous addresses, S.I.N. number and any other information describing the identity or personal situation and history of the taxpayer. It may be argued that this information is necessary in order that the Department of National Revenue be able to make a positive identification of the taxpayer and in at least that sense it is information obtained "for the purposes of the Act." Indeed, that was the conclusion reached by the Ontario Court of Appeal in a recent case, *Glover* v. *Glover*[5] The reasons for decision in that case said:

> The address of the taxpayer is a necessary and integral part of the information sought and received for the purposes of the Income Tax Act. To deliberately misstate the address is an offence under the Act. The section does not allow the Court to weigh the quality or relative value of the information. It prohibits the communication of "*any*" information received for the purposes of the *Income Tax Act*. In my opinion, the address received by the Minister of taxpayers on the Income Tax returns is information obtained by or on behalf of the Minister for the purposes of the *Income Tax Act*. Such information can only be communicated to persons authorized to receive it by virtue of the exceptions or qualifications contained in s.241.

41. We accept that analysis and proceed on the basis that it is correct. May an "official" or "authorized person" use information covered by section 241 to pursue an investigation or proceed with the prosecution of an offence unrelated to the Income Tax Act? Before the 1966 Amendments, which resulted in the current section 241, various court decisions held that in certain circumstances tax information could be used in a court of law, since the prohibition applied only to administrative and not to judicial proceedings. A judge sitting in a court of law was seen to be a person legally entitled to the information within the meaning of the section of the Act. The 1966 amendments indicate that no official or authorized person shall be required, in connection with any legal proceedings, to communicate or to give evidence of any tax information or produce tax records obtained for the purpose of the Act, unless such communication or testimony is in respect of criminal proceedings under a Federal statute, or in respect of proceedings relating to the administration or enforcement of the Income Tax Act (Section 241(3)). Despite the exclusion in subsection 3, of a reference to other civil proceedings, subsection 4(c) indicates that:

> (4) An official or authorized person may... (c) communicate...[tax] information... or allow inspection of or access to any book, or other [tax] document...*to or by any person otherwise legally entitled thereto.*
>
> (Emphasis is ours.)

In *Glover* v. *Glover*[6] it has now been held that a court is not a "person otherwise legally entitled thereto".

---

[5] *Glover* v. *Glover*, [1980] D.T.C. 6262 (Ont. C.A.).

[6] *Ibid.*

42. However, apart from the question of whether a court is entitled to have such information, there has as yet been no judicial interpretation of the section as to whether a member of the R.C.M.P. who is given the information for purposes, as far as the Revenue official is concerned, of the administration of the Income Tax Act, may use the information in *his own* investigation of an offence unrelated to the Act. We think the Act does not prohibit such a use. However, if he communicates the information to another member of the R.C.M.P. or a member of another police force, we do not think that he may lawfully do so, for he is then not making the disclosure for the purpose of the Act. If, as was held in *Glover* v. *Glover*, the court is not entitled, we cannot see that a policeman conducting a criminal investigation unrelated to the Act is entitled.[7] In Part X, Chapter 5, we shall recommend changes in the law so that the R.C.M.P. would have access to tax information to investigate offences unrelated to the Income Tax Act. Such access should be governed by a system involving judicial authorization, similar to that which now exists for the use of electronic surveillance. Whether the R.C.M.P. should be able to distribute tax information received under judicial authorization to other police forces is a matter for the Solicitor General of Canada to discuss with the provincial attorneys general.

43. Our conclusions are that:

(a) Furnishing of information, given to the Department by the taxpayer on his income tax return, to the R.C.M.P. for purposes other than enforcement of the Income Tax Act — for example, for a criminal investigation — is and has been a contravention of the Act on the part of any Departmental official communicating the information. If, in any of the specific cases, a member of the R.C.M.P. abetted (encouraged) the source, he was a party to the offence under section 21 of the Criminal Code. If he "counselled" or "procured" the source to commit it, he was a party to the offence under section 22 of the Criminal Code. We did not receive evidence as to such encouragement, counselling or procurement in specific cases. We note that the offence is a summary conviction offence; therefore there cannot be prosecution except within six months of the offence.

(b) No offence was committed if the information was communicated after the commencement of criminal proceedings.

(c) Furnishing such information to the R.C.M.P. for the purpose of the Income Tax Act, which was the express intention of the Memorandum of Understanding, was not in contravention of the Act.

(d) If any member of the R.C.M.P. who received such information passed it on to another member not engaged in an investigation relating to the enforcement of the Act, he may have committed an offence.

---

[7] This subject was also discussed by Mr. Justice Laycraft in his *Report of a Public Inquiry into Royal American Shows Inc. and its Activities in Alberta*, June 1978, at p. C-45.

C. UNEMPLOYMENT INSURANCE COMMISSION

44. Canadians are required by statute to provide information about themselves to the Unemployment Insurance Commission, both at the time of registering for a Social Insurance Number, and when applying for benefits. The Criminal Investigation Branch has been seeking access to this information to help to locate persons wanted for the commission of crime, to identify bodies and stolen property, and to find missing persons. In this section we give an account of the history, over 30 years, of the C.I.B.'s involvement with the U.I.C., and combine it with a discussion of the legal issues, for during that period there were several changes in the statute or in regulations, and it is therefore clearer and more convenient to mix fact and law.

1946 to 1965

45. There were no confidentiality provisions in the applicable statutes before 1946[8] and the transfer of information from the Unemployment Insurance Commission to the R.C.M.P. before that year raised no legal issues other than those that arise whenever a federal government employee gives official information to the police. In 1946 a confidentiality provision, section 105, was written into the Unemployment Insurance Act. It provided that

> Information, written or verbal, obtained by the Commission from any person pursuant to the provisions of this Act or any regulations made thereunder shall be made available only to the employees of the Commission in the course of their employment and such other persons as the Commission may deem advisable...[9]

Non-compliance with a requirement of the Act was made an offence in the same amendments and this has been a feature of the unemployment insurance legislation ever since. Therefore the release of confidential information to the R.C.M.P. was an offence unless the release complied with the requirement of section 105 that the Commission deem it advisable. It is clear from the evidence before us that members of the R.C.M.P. actively participated with personnel of the U.I.C. in obtaining confidential information after 1946, and therefore may have committed an offence of conspiracy to effect an unlawful purpose, contrary to section 423(2)(b) of the Criminal Code, or of abetting a person to commit an offence, contrary to section 21(1)(c) of the Code.

46. However, before it can be asserted that offences had in fact been committed, the following questions must be answered:

(a) Was it necessary that the discretion conferred by the confidentiality provision be exercised by the Unemployment Insurance Commission itself?

(b) If so, could the Commission delegate this discretion, and can it be proved to have done so?

(c) Could the discretion be exercised by an employee of the Commission, without authority to do so having been delegated by the Commission?

---

[8] See the Unemployment Insurance Act, 1940, S.C. 1939-40, ch.44.

[9] 1946 S.C., ch.68.

47. The first record of R.C.M.P. policy on the matter dates from December 1950, when members of the Force were permitted to seek information from the U.I.C. at its regional offices about individuals "who are being sought on criminal grounds and also respecting missing persons" (Vol. 57, pp. 9354-5). This policy was based on a letter dated December 9, 1950, from the Executive Director of the U.I.C. to the R.C.M.P. (Vol. 57, pp. 9352-3). A senior officer of the R.C.M.P. advised the officer in charge of the C.I.B. and the officer in charge of the Identification Branch that it would be "well to refer to the Commission only those cases where other enquiries are not productive" (Ex. H-1, p. 12). The policy became part of the R.C.M.P. Policy Manual in about 1964. In the same year the Social Insurance Number (S.I.N.) system was introduced by regulation[10] under both the Unemployment Insurance Act and the Canada Pension Plan Act. On June 4, 1964, the Ontario Division advised the U.I.C. that they would seek "information on the holder of a U.I.C. number and/or a new Social Insurance Number" (Ex. H-1, p. 15). Yet at or about this time the question was raised in the House of Commons as to whether information on a social registration card would be be made available to the R.C.M.P. On June 5, 1964 the then Commissioner of the R.C.M.P. wrote to the Minister of Justice, advising him that the Force was not using the information from the social security registration system and had no intention of seeking access to it (Vol. 57, pp. 9367-73).

48. On June 11, 1964, a Deputy Commissioner wrote to the Commanding Officers of all R.C.M.P. divisions advising them that the Commissioner of the R.C.M.P. had assured the Minister of Justice that the Force had no intention of seeking access to the information compiled during the social security registration programme and that "In line with this policy, no attempts are to be made by any member of the Force to obtain access to this material". Copies of this letter were sent to the Director of Security and Intelligence and the Director of Criminal Investigations (Ex. H-1, p. 16; Vol. 57, p. 9378). Two weeks later, however, the same Deputy Commissioner wrote a further memorandum to the Commanding Officers of all divisions (Ex. H-1, p. 17) which stated that access to the U.I.C. records was to continue whether the information had been given to the U.I.C. under the old alphabetical prefix system or the new number prefix system (Vol. 57, pp. 9392-3).

1965 to 1971

49. In 1965 the Canada Pension Act[11] was enacted. Sections 100 to 106 of this statute required that persons in "pensionable employment" file an application with "the Minister" for a Social Insurance Number. This provision cast a far larger net than the Unemployment Insurance Commission Act since it also covered self-employed persons. Section 107 of this statute contains the confidentiality provisions. These provisions differed considerably from the confidentiality section of the Unemployment Insurance Commission Act. Section 107 restricted the release of S.I.N. information compiled under that Act and would

[10] See P.C. 1964-379; (S.O.R./64-108).
[11] S.C. 1964-1965, ch.51.

prohibit the release of information to the R.C.M.P. for the purpose of law enforcement at large.

50. The C.P.P. (S.I.N.) Regulations[12] were enacted on August 11, 1965. These Regulations provided that a person required to apply to the Minister for a S.I.N. under the Canada Pension Plan Act was to do so by delivering or mailing his or her application to the local office of the U.I.C. (section 3(1)).

51. The evidence discloses that the S.I.N. information obtained by the U.I.C. under the provisions of the Canada Pension Plan Act was compiled in the Central Index of the U.I.C. The evidence shows also that the U.I.C. made no attempt to segregate Unemployment Insurance Commission Act information and Canada Pension Plan Act information in its Central Index, and responded to all requests by the R.C.M.P. for S.I.N. information.

52. While there is some evidence that the Force, including the Commissioner and Deputy Commissioner, were aware of the two different sources of S.I.N. information, there is no evidence that the Force was aware of the different confidentiality provisions in the two statutes. However, the evidence shows that the Force sought no legal opinion concerning these issues at any time during this period. According to the testimony of Assistant Commissioner Jensen, he always considered the matter to be an administrative, rather than a legal, concern. It is not unfair to interpret this view to mean that, as long as an employee of the U.I.C. in an apparent position of responsibility was prepared to release information, the R.C.M.P. would use it for the purpose of law enforcement generally.

53. In new instructions to members of the Force in 1967 reference was made for the first time to the Central Index of the U.I.C. It stated that requests for record checks could be made by divisions, branches, etc. to the U.I.C. offices and/or Central Index at Ottawa.

54. In June 1969 the Chief Supervisor of the Central Index of the U.I.C. advised by letter that he had no objection to R.C.M.P. field divisions sending requests for information directly to the Central Index by telex, and the R.C.M.P. Policy Manual was amended accordingly. The amendment advised that any telex message should indicate that the information was "being sought in connection with a criminal offence". It was clear in this policy that Social Insurance Numbers could be used. However, the Minister of Justice was not advised that the Force's position was now different from that which had been stated by the Commissioner to the Minister on June 5, 1964 (Vol. 57, p. 9405).

1971 to 1977

55. From early in 1971 until the fall of 1972 the formal flow of information from the U.I.C.'s Central Index was considerably restricted, to the point that it was all but terminated (Ex. H-1; Vol. 57, pp. 9408-23; Vol. 60, pp. 9827-8). In 1971 the Unemployment Insurance Commission Act was under debate in the House of Commons. It appears from the record that the restriction may have resulted from these debates; it was certainly contemporaneous.

[12] P.C. 1965-1458; (S.O.R./65-372).

56. The Unemployment Insurance Commission Act, 1971, assented to on June 23, 1971, carried forward the confidentiality provision previously found in section 105, in what now became section 114.[13] However, the statute elevated the U.I.C.'s S.I.N. registration system from the status of Regulations to that of a statute (see sections 125 and 126). With this elevation came a new confidentiality section, section 126(4), which provides as follows:

> (4) The Commission may, subject to such regulations as the Governor-in-Council may make in that behalf, make available such information contained in the registers maintained under section 125 or this section as the Commission deems necessary for the accurate identification of individuals and for the effective use by such individuals of Social Insurance Numbers and Social Insurance Number Cards, to such persons as the Commission thinks appropriate to accomplish such purpose.

This confidentiality section, rather than section 114, clearly applies to Central Index information (viz: S.I.N. information).

57. In August of 1972 the R.C.M.P. was made aware of the existence of section 126(4) and in fact was advised that that section in part was the reason for the change in position by U.I.C. personnel (Ex. H-1, p. 37).

58. Up to this time it appears from the record that the R.C.M.P. took the view that the predecessors of section 114 applied and took the further position that the question whether the R.C.M.P. were persons whom the Commission deemed "advisable" was an administrative issue, not a legal one. However, at this point the R.C.M.P. did not seek a legal opinion. Instead it either continued to assume that section 114 applied or was content to rely upon whatever "administrative" decision was made by the employee of the U.I.C. with whom it was dealing at the time.

59. In August and September 1972 the Executive Director of the U.I.C. confirmed that the R.C.M.P.'s operations manual provisions as to access to U.I.C. Central Index information "is acceptable to me but of course this does not constitute the Commission's policy..." (Ex. H-1, p. 42). The R.C.M.P. manual was amended in October 1972, in such a way that members of the Force were aware that information from the Central Index was again available. There is no evidence that the Unemployment Insurance Commission itself ever approved the arrangement (Vol. 57, pp. 9431-4). Enquiries were to be limited to certain specific major crimes "or any other serious crime" (Ex. H-1, p. 41). Assistant Commissioner Jensen told us that the words "serious crime" would mean any indictable offence under the Criminal Code or any federal statute (Vol. 57, pp. 9438-40). R.C.M.P. Headquarters sought information in regard to any type of "crime" until late 1976. At that time, as a member of the R.C.M.P. testified before us, information was to be requested only when it related to a crime on the list found in the 1972 arrangement or any other cases approved by a specific regular member of the Force at Headquarters (Vol. 58, pp. 9564-71). The witness testified that indeed the policy permitted the Force to obtain information for "some other purpose that is considered to be in the public interest": this included Security Service matters, missing persons and

[13] S.C. 1970-71-72, ch.48.

deceased persons (Vol. 58, pp. 9504-11), and information to assist other police forces or agencies (Vol. 58, pp. 9597-9606). These instructions differed from those agreed to by the Executive Director of the U.I.C., who had agreed to provide information only when the act being investigated "gives rise to a good deal of public indignation". Assistant Commissioner Jensen expected that R.C.M.P. personnel would have exercised discretion as to when to seek information (Vol. 57, pp. 9439-43).

60. The next major development in R.C.M.P. policy resulted from an agreement with the Chief of Benefit Control of the U.I.C. By a memorandum of September 10, 1973, Commanding Officers were advised that "This is a confidential verbal agreement we have with the Special Investigations Committee and therefore it should not be widely publicized...". The ability to obtain information from the U.I.C. was not to be disclosed "to anyone outside the Force" (Vol. 57, pp. 9490-1).

61. The next document that gave rise to a change in policy was a memorandum of October 3, 1973, to the Commanding Officers of all field divisions and to the Director General of the Security Service (Ex. H-1, p. 63; Vol. 58, pp. 9506-7). This memorandum removed all restrictions concerning the crimes with respect to which the R.C.M.P. could seek information from the U.I.C. Assistant Commissioner Jensen testified that, although he was unaware of any particular document that supported his understanding that the U.I.C. had agreed to this change, this was his recollection as to what the Chief of Benefit Control had agreed to (Vol. 57, pp. 9507-8). There is evidence, however, that this officer of the U.I.C. expected that information would be given only in "major cases" (Ex. HC-1, p. 32), and that he preferred all requests to be made by R.C.M.P. Headquarters to the staff of the U.I.C. Special Investigation Committee. Headquarters, in a memorandum to Commanding Officers, stated that "any sub rosa arrangements which may exist" were not to be interfered with (Ex. H-1, p. 63; Vol. 58, pp. 9550-2). This memorandum represents the policy as it stood when we held hearings into this subject in June 1978.

62. Section 126(4) is capable of two interpretations, namely:

(a) the Commission has no authority to release information unless such authority is granted by regulations enacted by the Governor in Council; or

(b) the Commission has authority to release information unless the Governor in Council enacts regulations to limit this authority.

63. Both these interpretations give rise to other problems of interpretation concerning the meaning of "accurate" identification of individuals. Is this phrase intended to help the Commission or law enforcement bodies in determining whether the individual using the card is entitled to do so under the provisions of the statute? Or is the phrase intended to help in the general identification of persons for any reason whatsoever? The former interprets the purpose of section 126 (4) as related solely to the use of S.I.N. information or cards in the social security system. This is supported by the evidence: the S.I.N. "... has been developed solely in connection with social security programs" (Ex. H-11).

64. The second interpretation of the phrase "accurate identification of individuals" would allow release of information, not only to law enforcement agencies but also to banks, retail stores, credit agencies, and any other persons or organizations. This broader meaning could be rationally supported if one believes that the legislators in 1971 accepted the following: that S.I.N. had become a national identification system and, consequently, that use of S.I.N. or a S.I.N. card was for purposes some of which went beyond the social security system.

65. If the correct interpretation is that the information can be released only for accurate identification of individuals or the effective use by individuals of S.I.N. numbers and cards, both for purposes of the statute, then the release of the Central Index information by the Commission staff to the R.C.M.P. subsequent to the Unemployment Insurance Commission Act, 1971, was contrary to law unless it was released for the purpose of enforcing the provisions of that statute.

66. Even if the broader interpretation, i.e., the identification of individuals for any purpose whatever, is correct, a legal problem exists. It is clear on the evidence that the 1972 and 1973 arrangements, which we shall describe shortly, contemplated the release of information to the R.C.M.P. for the investigation of either certain specified crimes or "crime" generally. The evidence before us shows that the use of the information was not restricted to "the accurate identification of individuals" or to the investigation of breaches of the Unemployment Insurance Commission Act. True, in some cases, the information was used by the R.C.M.P. to identify dead bodies and the use of a S.I.N. Card by a person other than the person to whom it was lawfully issued. However, it was also used in a considerable number of cases to locate wanted persons and in this regard was described by Assistant Commissioner Jensen as a necessary tool in the location of fugitives — "people who are sought on criminal grounds" (Vol. 57, pp. 9318, 9286, 9324; Vol. 58, p. 9657).

67. On May 10, 1973, the R.C.M.P. advised their personnel that the fact that it could obtain information from the U.I.C. was not to be disclosed to outside agencies or police departments and that any requests for information from these bodies were to be denied (Ex. H-1, p. 55). This policy was in effect confirmed by the memorandum of September 10, 1973, which has already been mentioned. It is therefore surprising that the evidence discloses that after 1973 the R.C.M.P. used its arrangement with the U.I.C. to provide information to other domestic and foreign agencies and police departments. There is no evidence that the U.I.C. or its employees did not know that the arrangement was being used for those purposes. The evidence is that the U.I.C. did itself provide information to outside agencies and other police forces prior to 1971 but not thereafter.

68. A further legal issue raised by section 126(4) is as follows. It provides that "The Commission may... make available such information... to *such persons* as the Commission thinks appropriate to accomplish such purpose". Can the Commission or its employees be said to have exercised its discretion if

it was unaware of the identity of the recipient of that discretion? We think it cannot.

69. A further legal problem arises on the facts. The R.C.M.P. was provided with information from regional offices of the U.I.C. from the beginning of the U.I.C. programme in Canada to June 12, 1978 (Vol. 57, pp. 9289-90, 9324-5). From at least 1972 onwards there is no suggestion on the evidence that the arrangements negotiated with U.I.C. personnel related to anything other than Central Index information: the obtaining of information from regional offices after 1972 was not according to any agreement with U.I.C. personnel. As a result the release of this information cannot possibly be said to have been provided for under section 114 or its predecessor, unless one interprets that section as permitting the release of information by *an employee* of the Commission — an interpretation which we think is unsound.

1977

70. Effective August 15, 1977, the statute was amended by the Employment and Immigration Reorganization Act,[14] (the "Reorganization Act"). It created a department known as the Department of Employment and Immigration, under the jurisdiction of the Minister of Employment and Immigration. Pursuant to this Act, section 114 was amended in one significant particular: responsibility for determining which "other persons" may share information under that section is now assigned to the Minister of Employment and Immigration. Thus, the concluding language of the confidentiality provision in section 114 now reads "and such other persons as the *Minister* deems advisable". (The emphasis is ours.) Moreover, the section now applies to information collected both by the Unemployment Insurance Commission and the Department of Employment and Immigration. The section authorizes release of that information to employees of the Commission *or the Department of Employment and Immigration* in the course of their employment and "such other persons as the *Minister* may advise". (The emphasis is ours.)

71. The terms of section 126(4) were, however, identical in the amendment. Thus, the Commission remains vested with the discretion to determine "such persons" as are appropriate to accomplish the "purpose" set out in section 126(4). While the comments previously made concerning section 126(4) continue to apply with respect to section 114, regard must be paid to a new delegation of authority section introduced by the Reorganization Act. Section 5(2) provides as follows:

> Except as provided in any other Act of Parliament the Minister may, by order, authorize any officers or employees of the Department [of Employment and Immigration] or the Canada Employment and Immigration Commission established by section 7 to exercise powers or perform duties and functions of the Minister and any such officers or employees or classes thereof specified in the order may exercise the powers or perform the duties and functions mentioned in the order.

[14] S.C. 1976-77, ch.54, assented to August 5, 1977.

Thus, section 5(2) permits the Minister to delegate the discretion he has under section 114 to the Commission or to the Department or to employees of either body. Such employees or classes of employees must, in accordance with the terms of section 5(2), be expressly designated in the Minister's order and, further, the powers or duties and functions to be performed by them must also be expressly referred to in the order.

72. There is no longer any doubt that the Commission may delegate its power of decision. On the other hand, the new power of delegation excludes any possibility that an employee of the Commission could lawfully release information in the absence of an express delegation. This conclusion is further supported by the provisions of section 13(3) of the Reorganization Act, which empowers the Commission, by order, to authorize:

> (i) any officers or employees or classes of officers or employees of the Commission,
>
> or
>
> (ii) with the approval of the Minister, of the Department,
>
> to exercise powers or perform duties and functions of or delegated to the Commission.

73. Section 9(2) of the Reorganization Act reads as follows:

> The Commission shall comply with any directions from time to time given to it by the Minister respecting the exercise or performance of its powers, duties and functions.

This section is relevant to the Commission's authority under section 126(4). It permits the Minister to direct the Commission to release information under section 126(4) provided always that the release is for the purposes set out in that section.

74. We have been advised that, since the present Act came into effect in 1977, the Minister of Employment and Immigration has not delegated his authority under section 114 to the Commission or the Department or their employees, or issued any direction to the Commission pursuant to section 9(2) with respect to the release of information pursuant to section 126(4). Finally, there is no evidence before us to suggest that the Commission in turn has sub-delegated its discretion under section 126(4) to any of its own employees, to the Department or to employees of the Department. Consequently, if there was no such sub-delegation by the Commission, in our opinion any release of information between August 15, 1977 and the cut-off of information imposed on June 12, 1978, may have been in violation of the statute.

75. On June 12, 1978, a representative of the Canada Employment and Immigration Commission advised the D.C.I. that the Force's access to Central Index Information was terminated (Vol. 57, p. 9240). The extent of the restriction on the information flow and the reason for the restriction is found in an excerpt from the House of Commons debates of June 21, 1978, which reads as follows:

> Mr. Bill Clarke (Vancouver Quadra): Mr. Speaker, my question is for the Minister of Employment and Immigration. I want to ask him about the

recently revealed refusal to supply unemployment insurance information to the R.C.M.P. In view of the fact that this information has been supplied for many years, in spite of the regulation regarding the confidentiality of unemployment insurance information, I ask what type of confidential information was supplied to the R.C.M.P. and under what authority was that information given?

Hon. Bud Cullen (Minister of Employment and Immigration): Mr. Speaker, the legal opinion I received recently indicated that in the past the information given to the R.C.M.P. went beyond that which was allowed under section 126. This was a legal interpretation of that section. It seems to me that it is open to interpretation. Because we wanted to get the matter clarified, it seemed the wisest policy was to issue instructions that information other than that for the administration of the Unemployment Insurance Act or the administration of social insurance numbers should not be released until we had clarification of section 126. I am happy that the McDonald Commission is looking into this particular area to give us advice either that we do have authority to give additional information as the minister shall determine, or that we should amend legislation to do what I think is appropriate, that is, to give this information to the R.C.M.P. to help their investigations.

Mr. Clarke: Mr. Speaker, I ask the minister what recent developments caused the ruling to be investigated and forced the government to stop giving that information.

Mr. Cullen: Mr. Speaker, until the carping of opposition members, we used what we thought was common sense and tried to help the R.C.M.P. in their fight against organized crime.

An hon. Member: Organized crime?

Mr. Cullen: I might say that with the passage of Bill C-27, the hon. member's colleague, the hon. member for Hamilton West, quite correctly thought that the minister should have the responsibility for giving information under the Unemployment Insurance Act to other people, and insisted that the wording be changed from "the commission" to "the minister" so that the minister had to accept responsibility. I sought a legal opinion to determine whether we were acting within the provisions of section 126. The advice I have from legal counsel is to the effect that more information is being provided than was authorized by that section. Because of that, I have ordered it stopped.[15]

76. For the reasons given above our conclusion is that throughout the three decades since 1946, the R.C.M.P. has obtained information from the staff of the U.I.C. by means which, through a failure to take advantage of the statutory provisions specifying the power of deciding upon access, have violated the confidentiality provisions of the legislation.

Extent and prevalence of access by the C.I.B. to U.I.C. data

77. The R.C.M.P. maintained Request for Information files from 1974 to April 1978. These files were created as a result of the 1973 arrangement and were maintained to record the requests that were made following the time of

[15] House of Commons, *Debates*, June 21, 1978, p. 6619.

that arrangement (Vol. 58, p. 9564). The requests for information made by the C.I.B. to the U.I.C. for the period 1974 to 1978 were as follows:

1974	—	265
1975	—	92
1976	—	544
1977	—	648
1978 (to April)	—	74
		1,623

Of the 648 requests for the year 1977, between 250 and 266 related to the investigations of U.I.C. frauds. Accordingly the number of non-U.I.C. related offences for 1977 was approximately 400 and for the period 1974 to April of 1978 was approximately 1,370 (Ex. H-7A; Vol. 60, pp. 9664-7). A review of the relevant files for the year 1976 and 1977 indicated as follows:

	Non-U.I.C. Recorded Requests	Reason for Request Not Indicated
1976	399	268
1977	428	313

78. The R.C.M.P. advised us that the request files are incomplete, and that the reason for the requests may have been communicated in a different fashion, for instance by telephone, by correspondence, or by reference to a particular case file. However, that information cannot be determined with any certainty at the present time (Vol. 58, pp. 9671-2).

79. The request files for the period 1974-78 indicate that other police forces and other agencies contacted the Commercial Crime Branch Headquarters computer terminal directly to make use of the 1973 arrangement. These included requests that were acted on from the following bodies, which are named here to illustrate the broad range of domestic and foreign forces and agencies whose requests were processed:

(a) Ingersoll Police Force
(b) Quebec Provincial Police Force
(c) Temagami Police Force
(d) Indiana State Police
(e) Winnipeg Police Force
(f) Medicine Hat Police Force
(g) York Regional Police Force
(h) Sudbury O.P.P.
(i) Kingston Police Force
(j) Burlington O.P.P.
(k) U.K. Customs
(l) Canadian National Railway Police
(m) D.N.R. — Collections Department

(Vol. 58, pp. 9600-4.)

D. OTHER FEDERAL GOVERNMENT DEPARTMENTS AND AGENCIES

(a) *Department of Industry, Trade and Commerce: the Industrial Research and Development Incentives Act*

80. Under the Industrial Research and Development Incentives Act,[16] known as I.R.D.I.A., the Minister of Industry, Trade and Commerce may authorize the payment of a development grant to a corporation for scientific research and development. A corporation applying for such a grant must provide such information as is specified by regulation and prescribed by the Minister. A statutory "privilege" is created by section 13, and disclosure of information contrary to section 13 is made an offence.

> 13. All information with respect to a corporation obtained by an officer or employee of Her Majesty in the course of the administration of this Act is privileged, and no such officer or employee shall knowingly, except as may be necessary for the purposes of sections 11 and 12 or in respect of proceedings relating to the administration or enforcement of this Act, communicate or allow to be communicated to any person not legally entitled thereto any such information or allow any such person to inspect or have access to any application or other writing containing any such information.
>
> 15.(2) Every officer or employee of Her Majesty who contravenes section 13 is guilty of an offence punishable on summary conviction.

Can the R.C.M.P. obtain access to such information? The references to sections 11 and 12 are irrelevant for our consideration as they relate to information obtained from the Minister of National Revenue or provided to that Minister. But what is the scope of the phrase "proceedings relating to the administration or enforcement of this Act", and when are members of the R.C.M.P. "legally entitled" to such information?

81. In 1974, the Commercial Crime Branch of the R.C.M.P., during the course of an investigation, wrote to the Deputy Minister of Industry, Trade and Commerce to obtain information concerning I.R.D.I.A. grants made by the Department to two firms. Apart from the existence and amount of grants, the Deputy Minister declined to provide information because of the provisions of section 13 of the Act. This resulted in contradictory legal opinions being given by the Legal Branch of the R.C.M.P. and by the Legal Services Branch of the Department. Finally, in May 1975, the Assistant Deputy Attorney General gave a written opinion that the Department may not, except pursuant to the exceptions contained in section 13, reveal to the R.C.M.P. information obtained under the statute. The Deputy Minister considered that opinion to be binding upon the Department but expressed willingness to co-operate by formally requesting an investigation pursuant to section 13 if the R.C.M.P. has information indicating possible irregularities in the administration of I.R.D.I.A.

---

[16] R.S.C. 1970, ch.I-10.

82. Such willingness to co-operate would apply only if the investigation related in a direct fashion to the Act. However, the investigation in question, in which the governing opinion was that information could not be provided, was under the Criminal Code. It concerned an allegation that an individual received a percentage of an I.R.D.I.A. grant in return for exercising his influence with the Government of Canada in regard to the application for the grant.

83. It appears from the documents before us (Ex. N-1) that on another occasion in 1974 a member of the Commercial Crime Branch conducting another investigation did obtain "complete access" to information in the files of the Department of Industry, Trade and Commerce, which had been obtained under I.R.D.I.A. There is no other evidence before us to indicate the extent and prevalence of such access. However, the Officer in Charge of the Operational Task Force (the group in the R.C.M.P. charged with tasks relating to this Commission of Inquiry and others) reported to us by letter dated November 21, 1978, that there was one case in 1975 in which there was an investigation of a possible "kick back" in regard to an application; that case resulted in the above-noted opinion being given by the Department of Justice. He added:

> Due to the fact that C.C.B. (Commercial Crime Branch) investigation files were not categorized by Government Departments, it would require a review of almost all Commercial Crime Branch files to determine if they dealt with an I.R.D.I.A. investigation. From speaking to members of C.C.B. they cannot recall any other case involving I.R.D.I.A.

We concluded that the time and cost of undertaking such a massive search were not warranted in the circumstances.

(b) *Department of National Health and Welfare: Family Allowances and Old Age Security*

84. Section 32 of the Family Allowances Regulations, 1954-1508, provided as follows:

> Except where required by law or when necessary for the administration of the Act or these regulations, no person who obtains information under the provisions of the Act or these regulations shall disclose or communicate such information or allow it to be disclosed or communicated.

85. The Family Allowances Act was repealed and replaced by The Family Allowances Act, 1973.[17] The confidentiality provision is now found in section 17 of the statute which provides as follows:

> (1) Except as provided in this section or section 18, all information with respect to any individual obtained by the Minister or an officer or employee of Her Majesty in the course of the administration of this Act and the regulations or the carrying out of an agreement entered into under Section 18 is privileged and no person shall knowingly, except as provided in this Act, communicate or allow to be communicated to any person not legally entitled thereto any such information or allow any person not legally entitled thereto to inspect or have access to any such information.

[17] S.C. 1973-74, ch.44.

The communication of such information contrary to section 17 is an offence:

> 20. (1) Every person who knowingly
>
> (e) contravenes section 17 by communicating or allowing to be communicated to any person privileged information or by allowing any person to inspect or have access to any statement or other writing containing any such information is guilty of an offence and liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding one thousand dollars or both.

However, subsection (2) provides a number of exceptions when information obtained by the Department in the course of the administration of the Act may be communicated to persons outside the Department. These exceptions are the Department of Indian Affairs and Northern Development, the Department of Manpower and Immigration, the Department of National Revenue, the Department of Supply and Services, the Unemployment Insurance Commission and Statistics Canada. The prohibition found in subsection (1) is also expressly not applicable to "proceedings relating to the administration and enforcement of this Act". Section 18 empowers the Minister to enter into an agreement with the government of a province under which the Minister may furnish to the government of a province any information which has been provided by a person who has applied for family allowances.

86. The "Minister" referred to in that Act is the Minister of National Health and Welfare. He is also the Minister referred to in the relevant provisions of the Old Age Security Act,[18] which have been in force since the Statutes of 1966-67. A similar prohibition was previously found in paragraph 3(1)(a) of the Regulations made pursuant to the previous Old Age Assistance Act. In that statute the confidentiality provision is found in section 19(1) which reads as follows:

> (1) Except as provided in this section, all information with respect to any individual applicant or beneficiary or the spouse of any applicant or beneficiary, obtained by an officer or employee of Her Majesty in the course of the administration of this Act is privileged, and no such officer or employee shall knowingly, except as provided in this Act, communicate or allow to be communicated to any person not legally entitled thereto any such information or allow any such person to inspect or have access to any statement or other writing containing any such information.

Subsection (2) provides a number of exceptions when information obtained by the Department pursuant to the Act or the regulations may be communicated outside the Department. These exceptions are the same Departments of the federal government as those referred to in the Family Allowances Act except that the Departments of Finance and Veterans' Affairs are added and the Departments of Indian Affairs and Northern Development and of Manpower and Immigration are not included. Information may also be provided to any provincial authority administering a programme of assistance payments. The prohibition found in subsection (1) is expressly not applicable to "proceedings relating to the administration or enforcement of this Act".

---

[18] R.S.C. 1970, ch.O-6.

87. The R.C.M.P. has long sought access to information provided to the Minister of National Health and Welfare by a parent applying for family allowances or a person applying for old age security. This information has been sought in order to assist individuals who have asked for the help of the R.C.M.P. in locating missing relatives and foreign embassies seeking persons, although the policy has been that, if such information is obtained, the person or embassy making the inquiry is not to be given the information if the "missing" person objects.

88. The R.C.M.P. has also sought the information in criminal investigations. For example, where a person suspected of a crime has vanished with his wife and children, information as to the address to which family allowance cheques are sent at the request of the parents may be of considerable assistance in enabling the police to locate the suspect.

89. In December 1954 R.C.M.P. Headquarters asked the Department of Justice for an opinion as to whether the furnishing of information to the Force to assist it in locating missing persons violated the "security" provisions of the Acts and regulations governing family allowances, old age security and old age assistance. In January 1955 the Deputy Attorney General, Mr. Varcoe, gave his written opinion that the provisions of the statutes and regulations

> preclude the giving of the information referred to therein to R.C.M. Police officers to assist them in locating missing persons. These prohibitions apply notwithstanding the manner in which a recipient proposes to deal with the information.

90. Consequently, in March 1955, a written instruction was sent to all divisions, sub-divisions and detachments. This advised of the ruling received from the Department of Justice. It then directed that members of the Force conducting enquiries as to the whereabouts of wanted or missing persons must not approach any regional office for information from the family allowances or old age security records. The instruction was entitled "Temporary" and was "to be withdrawn September 1, 1955". It was sent out as a "Temporary Instruction"

> . . . as it is felt that in six months time personnel in the field will be familiar with the fact that no information can be obtained from this Division of the Department of National Health and Welfare and a temporary instruction will have served our purposes.

91. In 1968 the officer in charge of the Commercial Fraud Section urged that an effort be made to overcome the "roadblock" created by the prohibition against disclosure that was then contained in a regulation under the Family Allowances Act, either by the Deputy Minister or another senior officer of the Department authorizing disclosure as a matter of policy, or by having the regulation amended. In order to prepare for an approach to the Department, the then Officer in Charge of the Criminal Investigation Branch, Superintendent M.J. Nadon, wrote to the Commanding Officers of the divisions to ask:

> which Divisions are suitable to acquire information through confidential sources within these Divisions

despite "the fact that they are statute [sic] barred by secrecy provisions within their regulations". The letter added:

> If we are receiving more co-operation at present than is apparent at this Headquarters, we may avoid any contact with the Department if we feel that such action would only serve to eliminate existing sources.

In reply, several commanding officers reported that information was being provided by confidential sources within the Department. Of these, the report from Alberta, by Detective Inspector T.S. Venner, explained that the assistance was being provided without the knowledge of the "national headquarters" of the Department and that he had been assured that "any official approach along these lines at Ottawa would only serve to eliminate these sources". The report from Manitoba was made by the member who obtained information from the Departmental source. It observed that the source had told him that the Regional Director of the Department

> continually brings to their attention the security aspects of their work and threatens dire results should there be any breach of same.

92. There is no indication that at that time any approach was made by R.C.M.P. Headquarters to the Department of National Health and Welfare. We infer that no approach was made for fear of affecting adversely the successful relationships that had been developed with sources within the Department in several provinces.

93. In November 1978 the Operational Task Force of the R.C.M.P., which had been created to carry out tasks related to Commissions of Inquiry, reported to us that it had conducted a survey of all divisions to determine whether local arrangements were in effect enabling members of the Force to obtain family allowance information. The divisions generally replied that as far as they could ascertain there did not exist any confidential arrangements with the Family Allowances Division of the Department. However, four cases were reported in which approaches were made by the Force to the Family Allowances Division other than in regard to the administration of the Family Allowances Act.

(i) In an investigation of the abduction of a seven-year-old child, the approach was made to determine whether a new application had been made for family allowance in regard to the abducted child. The Department advised that no new application had been made. (The mere disclosure that an application had or had not been made would not be prohibited.)

(ii) In 1970 co-operation was received in regard to a murder investigation. No further details were given.

(iii) A contact was made with the local office in an investigation under the Immigration Act. No further details were given.

(iv) A request was made in a fraud investigation. It does not appear that any information was given out, the disclosure of which would be prohibited.

Those cases illustrate the variety of situations in which information would be of assistance in criminal investigations.

(c) *Foreign Investment Review Agency*

94. The Foreign Investment Review Agency (F.I.R.A.) was established pursuant to the provisions of the Foreign Investment Review Act.[19] The Agency is empowered to advise the Minister concerning applications for the sale of control in Canadian business enterprises to non-Canadians, or the establishment of a new business in Canada by non-Canadians. In the case of the sale of an existing business, the applicant is the Canadian business enterprise. The applicant must provide the Agency with detailed information about the Canadian business enterprise or the new business. Section 14(1) of the Act is the confidentiality provision, violation of which is an offence:

> 14. (1) Except as provided in this section, all information with respect to a person, business or proposed business obtained by the Minister or an officer or employee of Her Majesty in the course of the administration of this Act is privileged and no person shall knowingly, except as provided in this Act, communicate or allow to be communicated to any person not legally entitled thereto any such information or allow any person not legally entitled thereto to inspect or have access to any such information.

The only exception provided for in the remainder of the section, which could in any circumstances enable the R.C.M.P. to have access to such information, is in respect of "legal proceedings relating to the administration or enforcement of this Act".[20] (Even that exception may not permit disclosure until after an information has been laid.)

95. In 1977, in a major international fraud investigation relating to "finder's fees", the R.C.M.P. attempted to obtain information from F.I.R.A. but F.I.R.A. personnel refused to provide the information on the ground that it was confidential. This illustrates that it is in the investigation of commercial fraud cases that F.I.R.A.'s information would be useful. Later that year the R.C.M.P. recorded that an arrangement had been made orally to deal with requests by the R.C.M.P. for information "unofficially, on a case by case basis". The arrangement entered into appears to us to have contemplated the furnishing of information in violation of the Act. However, so far as we have been able to ascertain the R.C.M.P. has not since then obtained any such information.

E. NEED AND RECOMMENDATIONS

96. In Part X, Chapter 5, we shall recommend that the R.C.M.P., for criminal investigation purposes, should have access to all personal information held by the federal government with the exception of census information collected by Statistics Canada. This access will be subject to a rigorous set of controls and review. Specifically we shall propose that R.C.M.P. access to personal information other than of a biographical nature be through a system of judicially granted authorizations subject to the same terms and conditions as are now found in section 178 of the Criminal Code with regard to electronic surveillance.

---

[19] S.C. 1973-74, ch.46.

[20] Section 14(4)(a).

CHAPTER 6

ACCESS TO AND USE OF CONFIDENTIAL INFORMATION HELD BY THE FEDERAL GOVERNMENT — SECURITY SERVICE

A. ORIGIN, NATURE AND PURPOSES OF PRACTICES

1. Members of the Security Service consider that important aspects of their work have been helped by having access to government information about individuals. Persistent efforts have been made to develop sources within government departments, whether in Ottawa or at some other centre. The Security Service members who developed these sources were, so far as can be determined from examination of the files, usually quite conscious that the sources would be breaking the law by contravening provisions of statutes concerning confidentiality of information. However, the Security Service considered that such information was needed to protect the security of Canada, and would be difficult and often impossible to obtain by other means. The sources themselves agreed to provide the information for entirely unselfish motives, being persuaded of the desirability and necessity of providing this form of assistance to the R.C.M.P.

2. As with the C.I.B. in Chapter 5, we shall examine the extent to which the Security Service gained access to several distinct sets of government records.

B. DEPARTMENT OF NATIONAL REVENUE

Policy and implementation

(a) *History*

3. During the Second World War, a regulation[1] made pursuant to the War Measures Act on July 30, 1940, made it mandatory that the Commissioner of Income Tax allow the R.C.M.P. to have access to any information contained in any return or other written document furnished under the provisions of the Act. This regulation was revoked on July 23, 1946.

4. Nevertheless, it appears that the Special Branch (which later became the Security Service) continued to have access to such information. On September 12, 1951, Superintendent (later Commissioner) McClellan advised the R.C.M.P. divisions across the country that thenceforth inquiries, which previ-

[1] P.C. 3563.

ously had apparently been directed to district offices of the Income Tax Branch, should be directed to R.C.M.P. Headquarters, so that Headquarters might ask the Income Tax Branch for information regarding the financial structure of an organization or the circumstances of an individual. Superintendent McClellan stated that the Income Tax Branch had indicated that statutory restrictions on the dissemination of information contained in Income Tax Branch files made the matter "rather delicate, not only from the legal viewpoint, but because of the fact it places employees of that branch in a rather difficult position".

5. Although there are no details in R.C.M.P. files of the relationship during the next 15 years, a memorandum on October 5, 1967, from an R.C.M.P. officer to the Director of Security and Intelligence, Assistant Commissioner Higgitt, stated that in November 1966, the Security and Intelligence Directorate's source in the Department of National Revenue had become increasingly concerned about co-operating with the R.C.M.P. The source had based his unwillingness to continue his co-operation on the fact that he was contravening the provisions of the Income Tax Act. The memorandum concluded that the source had been uncooperative for several months and appeared to be no longer available. Until this time, according to another memorandum, the source had provided information as to taxpayers' financial standing and other data which appeared on income tax returns. In this memorandum, the officer again recognized that a source, by co-operating, would be in contravention of section 133 of the Income Tax Act. On January 19, 1968, this officer wrote a memorandum in which he accepted that the provision of such information clearly resulted in a contravention of the Income Tax Act, and therefore it would be undesirable to obtain a ruling from the Department of Justice which could only state that the R.C.M.P. was excluded from obtaining the information. That, according to the officer, would then place the Security and Intelligence Directorate in the position that, if it carried on as it had in the past, it would be doing so "in contravention of a recent and explicit ruling from the legal officer of the Crown".

6. On October 24, 1969, after publication of the Report of the Royal Commission on Security, an R.C.M.P. memorandum suggested that renewed efforts should be made to establish liaison with the Department of National Revenue (Income Tax and Canada Pension Plan Divisions) and the Department of National Health and Welfare, "making the necessary submissions through the Solicitor General".

7. A memorandum by an R.C.M.P. officer dated November 18, 1969, noted the following passages in the Report of the Royal Commission, pertaining to the R.C.M.P.'s general relations with government concerning security matters:

> We have little sympathy with the more extreme suggestion that inquiries about persons should not be undertaken because of the individual's 'right of privacy', nor with the view that the process of personnel investigation by the State is alien to normal and democratic practice.

> Neither does an individual have a right to confidence; on the contrary, access to classified information is a privilege which the State has a right and duty to restrict.[2]
>
> Although the role of the R.C.M.P. is admittedly ill-defined, and recognizing that government policy has been inhibiting, we are not sure that the RCMP has made a sufficient, or a sufficiently sophisticated effort to acquaint the government with the dangers of inaction in certain fields. We are left with the impression that there has been some reluctance on their part to take desirable initiatives and some inadequacy in stating the case for necessary security measures in interdepartmental discussions at the higher policy-making levels.[3]

Obviously in these passages the Royal Commission intended to suggest that the R.C.M.P. should, in formal discussions of policy and amendments to legislation, be aggressive in emphasizing its need for information that would ordinarily be protected: the Royal Commission did not imply that the R.C.M.P. should make informal arrangements to obtain information by practices that resulted in violations of provisions of statutes.

8. However, it appears that even before that suggestion of such a formal approach was made, the Security Service had taken its own initiative. According to a November memorandum, the Service had, "in recent months, established a rather tenuous and highly restricted relationship with [source X] of the Income Tax Branch". (X is the name given by this Commission to a member of the Department of National Revenue, Income Tax Branch, who testified voluntarily to the Commission *in camera*. While much of that testimony was made public, the identity of X has been carefully protected by the Commission.) The memorandum continued that there was "the feeling that we cannot use this source to the degree that should be possible under more relaxed conditions, preferably generated from a more senior level". The memorandum also questioned the suggestion made of an approach through the Solicitor General, on the grounds that involving the Solicitor General would imply an attempt to amend the Income Tax Act, which would be self-defeating in that it would likely produce publicity, and that an unfavourable ruling by the Solicitor General would "effectively prevent us from subsequently attempting any alternative route". The memorandum suggested as an alternative that an approach be made to the Deputy Minister of National Revenue.

9. On November 25, 1969, in a note to the Director of Security and Intelligence, Assistant Commissioner Higgitt, it was recommended that Mr. Higgitt approach the Deputy Minister of National Revenue to explain the problem. If the Deputy Minister could not co-operate, the Security and Intelligence Directorate would somehow have to obtain the Solicitor General's good offices to intercede with the Minister of National Revenue. The note stated that "to continue efforts at any lower level simply puts these individuals on the spot". There is nothing in R.C.M.P. files to indicate that any meetings took place at or following that time between the Security and Intelligence

---

[2] *Royal Commission on Security*, 1969, paras. 79 and 80.

[3] *Ibid.*, para. 56.

Directorate and officials of the Department of National Revenue to establish a regularized practice of providing information to the Security and Intelligence Directorate.

10. While all these approaches were being exchanged, the relationship of the Security and Intelligence Directorate with X had been established. X received requests for two types of information: the first was "tombstone data", meaning such biographical information as the name and address of the taxpayer and his place of employment; the second was financial information. X agreed to provide information because X was convinced that it was necessary for the security of Canada. X's evidence was that X did not seek or obtain the approval of superiors, but acted independently, and we accept this evidence. X made the arrangements at a luncheon with R.C.M.P. officers, who explained the difficulties the R.C.M.P. were having in obtaining information about a certain class of persons of interest to the Security and Intelligence Directorate. X insisted that all requests be carefully screened prior to submission to X, that one R.C.M.P. officer deal only with X, that no communication be on paper so that no one in the Department would know what was going on, and that any information X gave to the R.C.M.P. officer not be disseminated outside the Security and Intelligence Directorate.

11. X testified to being aware of the provisions of Section 241 of the Income Tax Act. With respect to the tombstone data it had always been X's opinion that such information did not fall within the restrictions found in the section. With regard to financial data concerning the taxpayer, X was doubtful that providing the information was legal, and because of these doubts had insisted that all communications be oral. X did not anticipate that the Department of National Revenue would obtain any tax benefit in return for the release of tax information to the Security and Intelligence Directorate. X was unaware that at the time there was any consideration being given within the Security and Intelligence Directorate to obtaining official approval for access to tax information, and did not know that representations were being made by the R.C.M.P. concerning the matter.

12. The R.C.M.P. officer asked for and obtained, not only information which X could obtain from the computer, but also information which could only be obtained from the field. X recalled that this probably included information as to the source of income. In X's opinion, the Department of National Revenue should not be officially engaged in passing information on these grounds "because one of the cornerstones [of the administration of the Income Tax Act] was that we kept our files confidential". X testified that no one in the Department of National Revenue at that time knew that X was passing information to the R.C.M.P. Security Service. As far as X knew, no one other than the R.C.M.P. contact or the previous R.C.M.P. contact knew of X's identity as a source for the Security Service.

13. X told us that the Department's firm policy was to co-operate with no one at all unless there were legal grounds for doing so. If asked whether the Department could enter into an agreement with the Security Service or have anything to do with the provision of information to the Security Service, X's

advice would have been that that could not be done. Nevertheless, after listening to what the R.C.M.P. contact said, X felt prepared to accept the responsibility and risk of passing information, since the reasons for not passing information were outweighed by the difficulties the police were having in obtaining this type of information for what X considered "the security of the country".

14. X said that this was according to X's "own conscience, and my own belief in what Canada represented" and "that whatever it was, I wanted to protect that". X could foresee no tax advantage, and regarded the relationship not as being reciprocal, but rather as a one-way street. X acted out of a "sense of national duty". X admitted that when an individual in the Department of National Revenue decides in the interest of what he or she conceives a higher duty to the state, to give information obtained under the Income Tax Act to some body such as the police, "it certainly weakens the Department's image" and weakens the public confidence that tax information will be kept confidential. X never sought or received any payment for the services given to the Security Service, other than occasional lunches, and does not regret having made the decision to assist the Security Service.

15. We shall return to X later, but first it is necessary to refer to the evidence before us as to whether, in 1970, an agreement was made between another official of the Department of National Revenue and the Security Service for the passing of such information to the Security Service. On September 4, 1970, the R.C.M.P. officer who contacted X addressed a memorandum to the Commissioner, to the attention of the Director of Security and Intelligence, concerning contact X. (The code number rather than the name was used.) The memorandum reported that the officer had continued to see X frequently as and when required, and that X continued to cooperate freely and willingly. The memorandum reported that, while X had theretofore insisted on dealing personally with the writer, X had, however, that day "quite spontaneously and without any prior discussion" introduced the R.C.M.P. contact to Y, another member of the Department of National Revenue. The memorandum recorded that X very briefly explained to Y the nature of the relationship and told Y that if X was not available the R.C.M.P. officer could pass inquiries to Y, and Y would extend the same co-operation. The R.C.M.P. officer recorded that Y "quickly grasped the delicate nature of the relationship" and indicated the co-operation would be forthcoming. Mr. Starnes says that he does not think that he was aware of this September 4, 1970, memorandum.

16. On September 15, 1970, Mr. Starnes, in a longhand memo to Superintendent Chisholm, said:

> I spoke to Commissioner about this matter on 3 September. He told me the Minister was opposed to joining with his colleague the Minister of National Revenue in a submission to cabinet. Could a 'blind' memo on the present state of play be prepared which I could use in talking to the Minister.

17. On September 23, 1970, a longhand note by Mr. Starnes to the Commissioner stated:

> If you see no objection I would like to show this memo to Minister on next occasion we see him to try and get action on question of access for S & I purposes to income tax records.

The memorandum in question is one which related to the use to which such information would be put by the Director of Security and Intelligence. In a longhand note at the bottom of the memorandum dated September 23, 1970, Commissioner Higgitt stated:

> I have raised this a number of times with the Minister and will do so again. He has not as yet been able to get the Minister of National Revenue to give his Department the necessary instructions to cooperate even though he seems to be favourably inclined himself. Mr. Côté is seemingly facing considerable opposition from his departmental officials. I will raise it again. I have retained a copy.

Mr. Starnes testified that he has no recollection of having raised the matter with Mr. McIlraith.

18. (It will be recalled that, in connection with criminal investigations, Commissioner Higgitt had written to Mr. McIlraith on March 20, 1970, advising him that representatives of the D.N.R. and the R.C.M.P. had finalized a draft agreement and a Memorandum to Cabinet.)

19. On September 8, 1971, X's R.C.M.P. contact addressed a memo to the Commissioner, to the attention of the Director General of the Security Service, with regard to X, identifying X by code number. The memorandum recorded that X's contact and another R.C.M.P. officer had entertained the source at lunch on September 7, 1971, and that the other R.C.M.P. officer had been introduced to the source. He also recorded that they discussed with the source

> . . . the fact that the Solicitor General had elicited agreement from [a public servant in] the Department of National Revenue to provide the Security Service with information from Taxation Records; Source was fully aware of this and told us how [the source] had explained to the [public servant] that the arrangement would have to remain unofficial due to lack of a legal base for passing such information. Source's view is that [the source] now has approval from the source's [superior] to do what [the source] has been doing for us on [the source's] own initiative for the past two years.

The memorandum also indicated that the Security Service should continue to deal directly with X only. According to the memorandum of September 4, 1970, X had introduced the writer to Y, who was to be used as an alternative only when X was not available. The writer believes that his memorandum accurately set forth what happened (Vol. 147, pp. 22714-5). In a further memo of September 8, 1971, the writer also stated that X

> insists on confining the arrangement to these few people as there is no legal base for this activity thus leaving [the source's] department in an indefensible position should wider knowledge of the arrangement cause a leak into the public domain.

20. X confirmed to us having been introduced to another R.C.M.P. officer by the R.C.M.P. contact and thinks it was at a lunch meeting. X recalled that the R.C.M.P. contact was leaving his position and another R.C.M.P. officer was to

replace him. However, X denied having discussed with the R.C.M.P. contact that the Solicitor General had elicited agreement from a public servant of the Department of National Revenue to provide the Security Service with information from taxation records. X denied having discussed the matter with the person in the Department to whom the memorandum referred (Vol. 147, p. 22672).

21. X testified that X never told any public servant what X was doing in respect of this matter, and had no recollection of introducing Y or making the arrangement that Y would be a substitute. We accept the facts as set forth in the memorandum written by X's contact. X further said that as far as X knows, no one in the Department knew that X was passing information to the Security Service (Vol. 147, p. 22656).

22. The consciousness of senior officers of the Security Service across Canada that the practice was illegal is demonstrated by their honouring the request of Headquarters that a memorandum of August 19, 1971, concerning access to taxation records be returned for destruction.

23. Despite attempts by the R.C.M.P. contact to have all requests for taxation information routed through Headquarters, it appears that Security Service members at the local level continued to use local sources in the Department of National Revenue. On February 24, 1972, an R.C.M.P. memorandum for file, written by X's contact, noted that

> From the number of incidents appearing from the field of our members inadvertently using long established local sources in this area it is obvious that we are not going to be able to 'turn off' the field Divisions in this area without taking unnecessarily large issues [sic] on the subject.

His memorandum records that he proposed to the Acting Deputy Director General, on February 16, 1972, that he discuss the matter with X and that if X agreed, the R.C.M.P. contact would tell the divisions that it would be in order to resume discreet use of the local sources. The R.C.M.P. contact records that the Acting DDG agreed, that he spoke with the source on February 17, 1972, and that the source agreed, saying that there was no "need for [the Security Service] to persist in trying to prevent [its] members from contacting their local contacts". Consequently, on February 24, 1972, the R.C.M.P. contact wrote to the Commanding Officers across the country, advising that the local Department of National Revenue sources could be used discreetly.

24. The official Security Service policy was recorded in the policy manual, on a page dated April 19, 1972, as follows:

Liaison with Income Tax Branch

> Due to statutory restrictions imposed on information contained in Income Tax files it is usually not possible to obtain the desired information from district tax offices. Headquarters *may* be in a position to assist in this regard provided the enquiry is sufficiently important and there are no other sources from which to obtain the information. The specific information desired concerning the financial structure of an organization or individual must be stated in the requests to Headquarters.

25. X continued as a source at the Department of National Revenue in Ottawa until replaced by another (Ex. GC-11).

Extent and prevalence

26. A Staff Sergeant who since 1971 has been attached to the Branch of the Security Service which has responsibility for programmes of developing "human sources" testified that between August 1971 and the fall of 1977 he was able to ascertain 132 instances in which information was obtained from income tax files. Of these, 52 involved X's co-operation. The balance were either through Headquarters (presumably through X's successor as source) or through local contacts. He believes that divisions kept records of access from August 1971, when they were informed that an agreement had been reached in Ottawa. In late 1977 the association with the "main source" in Ottawa was stopped by the Security Service handler. No instructions were sent by Headquarters to the divisional level that the members of the Security Service were to desist from obtaining such information, and there is no evidence as to what has occurred at the local level since the fall of 1977.

27. So far as can be ascertained, no payment was ever made to, or expected by, sources in the Department of National Revenue.

Legal issues

28. An exposition of legal issues, as applicable to the Security Service, would be no different than the discussion already set forth in regard to the C.I.B. in Chapter 5. There is no need to repeat what is developed there.

29. If a court, engaged as was the court in *Glover* v. *Glover*,[4] in applying the law as to the custody of children, is not a person "legally entitled" to the address of a taxpayer, we think that a member of the R.C.M.P. Security Service cannot be said to be a "person legally entitled" to biographical information or financial information disclosed on an income tax return. If this is so, the disclosures made by sources in Ottawa or elsewhere were offences by those persons under section 241, and if in any of the specific cases, a member of the R.C.M.P. "abetted" (encouraged) the sources, he was a party to the offence under section 21 of the Criminal Code. If he "counselled" or "procured" the source to commit it, he was a party to the offence under section 22 of the Criminal Code. We did not receive evidence as to such encouragement, counselling or procurement in specific cases. If the Attorney General of Canada considers that further investigation of specific cases is desirable with a view to considering whether there should be prosecution, he may begin his investigation with some specific cases of which details of a general nature are given in our records. However, we note that the substantive offence is a summary conviction offence; therefore there cannot be prosecution except within six months of the offence.

[4] [1980] D.T.C. 6262 (Ont. C.A.). This case is discussed in Part III, Chapter 5.

C. UNEMPLOYMENT INSURANCE COMMISSION

Security Service Policy

1950-1964

30. Co-operation and information exchange between the Unemployment Insurance Commission and the Security and Intelligence Directorate of the R.C.M.P. initially developed out of the arrangements entered into between the C.I.B. and the U.I.C. Until 1956 the Special Branch (predecessor of the present Security Service) was part of the C.I.B. In 1956 it became the Directorate of Security and Intelligence and ceased to be part of the C.I.B. However, it "piggy-backed" on the C.I.B. arrangements to obtain biographical data and other information collected by local offices of the U.I.C. (Ex. H-1, p. 134; Vol. C16, pp. 7852-3).

31. It will be recalled from our narrative in Part III, Chapter 5, that the Deputy Commissioner of the Force wrote to the Commanding Officers of all divisions on June 11, 1964, to advise that the Commissioner of the Force had assured the Minister of Justice that the Force did not intend to seek access to confidential data which would be collected under social security legislation then before Parliament, and that members of the Force were therefore not to seek access to information accumulated by the U.I.C. under this programme (Ex. H-1, p. 16). This memorandum, a copy of which was circulated to the Director of Security and Intelligence, and retained in the files of the Security and Intelligence branch in Toronto, contained the following admonition: "This is forwarded for your information. Please see that all members under your command comply with the Deputy Commissioner's instructions" (Vol. C16, pp. 1861-2; Ex. HC-1, p. 72). However, as we have also seen, the Deputy Commissioner wrote a further letter on June 25, 1964, just two weeks later, instructing that access to U.I.C. records was to continue.

1964 to 1971

32. From August 1964 to March 1971, the Security and Intelligence branch at "A" Division in Ottawa had its own direct, person-to-person working relationship with a U.I.C. representative, pursuant to which the branch, through this representative, could gain access to the Master Index and obtain information from regional offices of the U.I.C. (Vol. C16, pp. 1858-60; Ex. HC-1, p.1). There was no arrangement between the Security and Intelligence Directorate at Headquarters and the U.I.C. during this period, although Headquarters was aware of the "A" Division arrangement (Vol. C16, pp. 1875, 1891-2). There is no indication on the evidence that the Security and Intelligence branch of any other division had such an arrangement with the U.I.C. during this period (Vol. C16, pp. 1863, 1870, 1872).

33. In March 1971 this flow of information to "A" Division was all but cut off by the U.I.C. in light of "questions in the House of Commons". Following this restriction the U.I.C. continued to supply a social insurance number when "A" Division could provide a name (Ex. HC-1, p. 8). This "cut-off" of information resulted in an exchange of correspondence at the ministerial level

between the Honourable Jean-Pierre Goyer (the Solicitor General) and the Honourable Bryce Mackasey (the Minister of Labour) following which meetings were arranged between U.I.C. and Security Service representatives to discuss the resumption of the flow of information.

1972 to 1978

34. On January 19, 1972, an official of the U.I.C. in Ottawa advised the Security Service that the information flow to the Security Service in "A" Division would be resumed. Two senior officers of the Security Service in "A" Division became the Security Service contacts with the U.I.C. (Exs. HC-1, pp. 5-6, 17, 28-30; HC-2, pp. 1-2).

35. This arrangement continued until the summer of 1973 when the Special Investigation Division (S.I.D.) of the U.I.C. made a new arrangement with the Security Service at Headquarters to create an information flow (Ex. HC-1, p. 32). The Security Service operated under this arrangement until June 12, 1978, and because of this new arrangement, "A" Division's relationship with the U.I.C. ceased (Vol. C16, p. 1940).

36. In addition to the Headquarters arrangement, working relationships existed between the local offices of the Security Service and the local offices of the U.I.C. These contacts were tolerated by the sources branch of the Security Service at Headquarters (Vol. C16, pp. 1949-50; Ex. HC-1, p. 61).

37. Finally, the evidence indicates that from October 30, 1973 until the fall of 1977 a quite distinct relationship existed between the Security Service at "O" Division in Toronto and employees of the U.I.C. offices there. The Security Service in Toronto could obtain information contained on social insurance application forms and then check it against the benefit records maintained by the U.I.C. on its National Claim Tape. The Security Service member could then contact the District Office of the U.I.C. to obtain further information (Vol. C16, pp. 1946, 1953, 1955-6; Ex. HC-1, pp. 52-53, 55, 62). With the disbanding of the S.I.D. at the U.I.C. in 1975, "O" Division's contact was directed to a contact at U.I.C. Headquarters in Ottawa. This direct contact ceased in the fall of 1977 (Vol. C16, pp. 1958-59, 1962).

38. There is one aspect of the correspondence between Ministers in 1971 which we wish to mention. At the request of Mr. Starnes, Mr. Goyer wrote to Mr. Mackasey, the Minister responsible for the U.I.C., requesting the co-operation of the U.I.C. On August 18, 1971, Mr. Mackasey replied to Mr. Goyer agreeing to the suggested meetings between the U.I.C. and the Security Service

> . . . to discuss this whole matter and to formulate a policy recommendation concerning all matters associated with the question, such as the Unemployment Insurance Act and Security Service requirements.

He also stated:

> . . . the provisions affecting the release of information from the Central Index of the Unemployment Insurance Commission have been modified somewhat under the new Unemployment Insurance Act. One of the pur-

poses, therefore, of the proposed meeting between the officials of our two Departments would be to review these new requirements in order to determine how the Commission can provide assistance to the R.C.M.P. within the framework of this new legislation.

(Ex. HC-2, p. 4.)

A meeting was held between representatives of the Security Service and the U.I.C. in October 1971 with the U.I.C. representative reported as stating he would have to discuss the matter "with others". On November 25, 1971, a memorandum written within the Security Service to the Security Service representative, as to what should be said in future discussions with the U.I.C. representative, stated:

> We suggest that in your discussions you subtly let him be aware of the fact that you know that *his Minister has agreed in principle to co-operate with the Force in this matter, without showing him the actual correspondence.*
>
> (Our emphasis added.)

Now, Mr. Mackasey's letter could not be read as "agreement in principle to co-operate with the Force in this matter" in the sense that he had agreed in any operative sense to provide information to the Force. One can readily infer that the reason for not showing the U.I.C. representative Mr. Mackasey's letter was that, without seeing it, the U.I.C. representative would more likely swallow the "subtly" communicated false information. Such an attitude by the R.C.M.P. toward another department of government is indefensible.

39. The only evidence as to whether, in 1972, the U.I.C. representative at the October meeting ever spoke to the Chairman of the U.I.C., is that of a member of the R.C.M.P. Indeed his evidence does not include any indication, even by hearsay, as to whether the U.I.C. official obtained any approval from anyone for the arrangement he entered into.

40. The association between the Security Service and U.I.C. was "never a point of concern from the point of view of legality" in so far as the Force was concerned (Vol. C16, p. 1966). Moreover, as far as was known by an officer of the Security Service who testified before us, the U.I.C. had not made it a "matter of legal concern". It is difficult to reconcile this position with a Security Service memorandum dated January 6, 1972, from a senior officer of the Security Service to the Deputy Director General, which recorded that at a meeting with a senior official of the U.I.C. the official had said that

> the matter could be raised verbally directly with the Chairman... who would decide whether or not it would have to be taken up with the Minister or whether an arrangement could be made for co-operation on a limited and sub rosa basis.

Anyone reading that memorandum's reference to co-operation on a "sub rosa basis" would be aware that there were problems.

Extent and prevalence

41. There is no evidence as to the extent to which information was provided by the U.I.C. to the Security Service at the divisional level of the R.C.M.P. However, the person at Headquarters who contacted the U.I.C. from the

summer of 1973 to September 1977, testified as to the extent to which Headquarters obtained, or attempted to obtain, information. In 1974 he made 127 requests, in 1975, 134 requests, in 1976 (the year of the Olympic Games in Montreal) he made 373 requests, and in 1977 567 requests. His successor made 136 requests from September 1977 to June 7, 1978. After June 12, 1978 no further requests were made (Vol. C16, pp. 1944-61, 1976).

Legal issues

42. The legal issues are identical to those discussed in connection with the C.I.B.

D. OTHER FEDERAL GOVERNMENT DEPARTMENTS AND AGENCIES

Department of National Health and Welfare: Family Allowances and Old Age Security

43. We did not inquire into whether the Security Service obtained access to family allowance and old age security information. We do know that, as in the case of access to information in the possession of other federal government departments, on July 27, 1971, Mr. Goyer, at the request of the R.C.M.P., wrote to the Minister of National Health and Welfare to request access to "the considerable biographical and other data on persons which is maintained in the Department of National Health and Welfare (Canada Pension Plan and Family Allowance and Old Age Security Divisions)", which he said "could be of great value to the Security Service in the discharge of its duties". The letter asked for interdepartmental discussions to determine "whether the requirements of the Security Service could be met within the framework of existing laws and regulations and in a manner which would attract no attention or criticism". In his reply of August 18, 1971, the Honourable John Munro, Minister of National Health and Welfare, wrote as follows:

> While I am sympathetic with the desire of the R.C.M.P. to reduce costs and improve efficiency in their operations, I am afraid that I would have to oppose in principle the use of data secured in connection with applications for Social Security benefits for any other reasons than to determine entitlement to those benefits.
>
> It has been our experience over the years in building up a structure of Social Security plans for Canadians that in order to secure the acceptance of the people of Canada of the various plans which have been introduced, one of the essentials is for them to have the assurance that the information they must provide will be kept in strict confidence, and will not be used for other purposes. This is reflected in the fact that in each of the laws which provides for the payment of social benefits there is a prohibition limiting our authority to disclose information obtained under the Act or the Regulations to situations where it is essential that this be done in order that the legislation may be properly administered.
>
> For any change to be made legislative action would be required, and I believe that even if we were not opposed in principle such amendments

> would not be acceptable to Canadians generally, particularly in the light of present conditions. As I indicated earlier, it is necessary for the people of Canada to accept the various laws if they are to be effective as approved by Parliament. There is no question in my mind, again apart altogether from the principle of the matter, that many persons, however much they might wish to receive certain benefits, would be reluctant to make application if they felt that the details they would have to provide concerning themselves and their families could be used against them in some other way.

(It may be noted that it was not strictly correct to say that "each of the laws" prohibits disclosure of information except "where it is essential that this be done in order that the legislation may be properly administered". For, as has been seen, the Old Age Security Act at the time already allowed information to be communicated to six other federal departments whose functions did not include administration of the Old Age Security Act.)

E. NEED AND RECOMMENDATIONS

44. In Part V, Chapter 4, we shall recommend that the security intelligence agency have access to the same federal government information as we propose for the R.C.M.P. in criminal investigations — that is, all personal information with the exception of census data collected and held by Statistics Canada. Our proposed system of controls to govern such access is similar to what we recommend for other highly intrusive investigatory methods. For personal information not merely of a biographical nature, the security intelligence agency would require the approval of the Solicitor General before making an application to a judge for a warrant.

CHAPTER 7

COUNTERING — SECURITY SERVICE

A. NATURE, ORIGIN AND PURPOSE OF DISRUPTIVE COUNTERING MEASURES

1. Some of the R.C.M.P. Security Service's practices which have involved activities not authorized or provided for by law have been referred to as 'countering activities'. There is considerable confusion as to what is included under countering activities. Some witnesses referred to the successful collection of intelligence about a security threat as a method of countering, but this usage is so elastic as to be meaningless. We prefer to limit the use of the word 'countering' to any positive steps that may be taken by the agency itself as a result of the collection and analysis of information, other than reporting intelligence to government. Some of these steps have traditionally been taken by other government departments or police forces rather than by the R.C.M.P. Security Service. Some of the measures taken by the Security Service have been unlawful. Of the lawful countermeasures, some have been of a nature that are appropriate to a security intelligence agency, while others in our view are not.

2. Some of the countermeasures undertaken by the Security Service have been regarded within the Service as 'disruptive', a phrase used to describe activities directed by the F.B.I. in the late 1960s against certain groups in the United States. A memorandum of June 11, 1971 (Ex. D-2), from the officer in charge of "G" Branch in Montreal, describes 'disruptive tactics' as follows:

> Making use of sophisticated and well researched plans built around existing situations such as, power struggles, love affairs, fraudulent use of funds, information on drug abuse, etc., to cause dissension and splintering of the separatist/terrorist groups.

Certainly this suggestion was at least partly inspired by belief that these tactics were in use in the United States, but since in a sense all countermeasures are 'disruptive' in their desired result, the word itself is unhelpful in assisting us to discriminate between acceptable and unacceptable countermeasures.

3. The use of tactics that, while not contrary to law, are intended to disrupt the effectiveness of a targetted organization, is not new. There is documentary evidence that the R.C.M.P., in 1956, distributed at least one letter among members of the Labour Progressive Party — a letter which was prepared by the R.C.M.P. as if it were written by a member of the Party and attacked the Soviet Union on a vital issue and the Soviet Communist Party's post-Stalin

leadership generally. The letter, which we saw, was reported to Commissioner Nicholson and Assistant Commissioner Harvison, both of whom had approved the operation, as having caused "definite concern and confusion within the Party ranks".

4. The national programme of 'disruptive' countermeasures from 1971 to 1974 under the code names ODDBALL and CHECKMATE, which is referred to in some detail later, was developed by a Special Operations Group at Headquarters. The officer in charge, who thereafter rose to a senior rank, stated in a memorandum in 1979 that

> (a) The use of calculated and measured security responses must be viewed in a historical perspective. Checkmate was developed and implemented as a proactive measure to contain or neutralize political violence at a time when such violence was rapidly increasing and accumulating. The lessons of the F.L.Q. crisis had indicated both to the government and to the Security Service that reactive or passive measures were not adequate. The government's invocation of the War Measures Act was a security response which it did not relish nor wish to use again. The onus to ensure this clearly fell within the mandate of the Security Service.
>
> (b) Checkmate was a calculated and measured security response aimed at containing or preventing the occurrence of political violence. It was strictly controlled to prevent abuses, but vigorously propagated to ensure results.
>
> (c) Many legal mechanisms in place at the time were either reactive and therefore inappropriate to intelligence needs, or were inadequate in terms of new security threats.

For these reasons he and the officers who served on the Special Operations Group consider that the countermeasures undertaken as part of this programme should be viewed against the background of the times. The reasons for the programme, as he described them in his testimony, can be summarized as follows:

(a) In the late 1960s the Security Service found itself faced by what it perceived to be an evolving threat to Canadian internal security which was different from the Communist threat which had been posed in the past. The new threat was seen as being a world-wide confrontation with authority by various groups employing violence for political ends.

(b) Violence erupted on the part of students and union members in France in 1968. Students battled police in the Federal Republic of Germany and Mexico. Mexican terrorists were recruited in Moscow and trained in North Korea. There was violence in the Middle East, and Palestinian violence began to spread elsewhere in the world. Palestinian terrorists began to work with the Japanese Red Army and the Baader-Meinhof gang. In 1972 the J.R.A. was responsible for a massacre at Lod Airport in Israel and the Baader-Meinhof gang supported the Palestinian Liberation Organization massacre at the Olympic Games in Munich. There was growing violence in South America. In the United States there were major confrontations, including acts of violence and bombings, by such groups as the Weather-

men and the Students for a Democratic Society. A strong and active black 'extremist' movement developed in the United States, including the formation of a Black Liberation Army, which was responsible for the killing of policemen in New York City.

(c) In Canada in the late 1960s and early 1970s there were growing numbers of confrontations and bombings, kidnappings and murder. The Security Service was concerned about what it saw as a growing black 'extremist' movement which was believed to have contacts with the black 'extremist' movement in the United States. Computers at Sir George Williams University were destroyed by students in 1969. The Security Service was also perturbed by small Marxist groups which it identified as New Left groups. These groups were considered to be responsible for demonstrations in which there were confrontations with the police. Some of these groups had contacts with groups in the United States. New Left activists from abroad, such as Daniel Cohn-Bendit and Jerry Rubin, visited Canada. The Security Service had a "major concern" that the New Left groups, the black 'extremists', the F.L.Q. "and the like" might form a common front. There was also an organization which was involved in 39 street confrontations and other incidents with the police, out of which arose 175 convictions. Palestinian activists visited Canada, contacted the F.L.Q., and provided guerrilla training to F.L.Q. members in the Middle East. Eight letter bombs addressed to Canada were intercepted outside Canada. The Security Service was also concerned with the Trotskyist movement which, at a World Congress in 1969, had approved the use of guerrilla warfare in South America. Canada and four other countries experienced the bombing of Yugoslav embassies and in Sweden the Yugoslav ambassador was murdered. Anti-Castro Cubans bombed Cuban mission premises in Ottawa and Montreal.

5. To meet some of these threats or perceived threats, Canadian police forces and the Department of National Defence were forming their own intelligence units. The police forces hoped thereby to develop evidence for the purpose of criminal prosecution. However, they found that prosecutions could rarely be launched or carried to a successful conclusion except when violent confrontation occurred on the streets. A feeling developed that, because the law could be applied only after offences were committed, the enforcement of the law was an inadequate means of effectively forestalling politically motivated acts of violence (Vol. 169, pp. 23254-5). Consequently, in 1970 the Security Service established the Special Operations Group, the purpose of which was to bring forward for the Countersubversion Branch innovative objectives and goals on a national basis. In 1971, this group acted upon what they understood to be the Director General's wish that there be more emphasis on containment, prevention and neutralization (Vol. 169, p. 23271). When discussing ODDBALL, an R.C.M.P. officer told the Group that they were to create programmes of disruptive measures where the target was of such a nature as to make such measures necessary. The limits were set first by the extent to which the operation was necessary, and second by the extent to which positive benefits could flow from the operation. There is no evidence before us of any consider-

ation having been given to whether operations should be within the law (Vol. 169, p. 23278). In June 1972, disruptive measures were authorized including "widespread harassment at every possible opportunity", against one Maoist group considered to be responsible for much violence. This was contemplated as consisting of the enforcement of by-laws and statutes, the execution of warrants, the initiation of deportation proceedings and the exploitation of rifts (Ex. PC-78, Tab 33). In March 1972, at a meeting of senior officers, Mr. Starnes urged that branches of the Security Service be "far more vigorous in their approach to disruptive activity" and promised his complete support for "well conceived operations". In a summary of the meeting, subsequently distributed by him, the "neutralization" of an organization or individual whose purposes were "clearly seen" to be "at cross-purposes with the maintenance of domestic stability" appeared as part of the discussion. Security Service officers in the field, said the memorandum, should not allow "reticence" to influence their work in disruptive operations, and if they failed to comply with tasks set for them by Headquarters, they "would be subject to censure, including, if necessary, transfer" (Ex. PC-78, Tab 26).

6. A senior member of the Special Operations Group considers that any CHECKMATE operations were proper "without any regard to whether they were... lawful or unlawful" as long as they were "responsible", "reasoned" and "measured". In his mind, any operations that met those criteria were as acceptable as a peace officer's interception of the driver of a speeding or recklessly speeding vehicle. He told us that in his basic training he was taught that the law permitted reasonable response when in other circumstances the same conduct would be illegal. He equated the emergency situation — the need to apprehend an offender who is committing an offence — with taking measures to bring an end to circumstances which, if unchecked, could lead to "the ascendency of violence" in Canada (Vol. 173, p. 23640).

7. If we may generalize from the case of this witness, an experienced member with a university degree, the early training of members of the R.C.M.P. as to what their powers are as peace officers appears to be significant. Such training had a bearing on the ability of members of the Security Service, in the early years of the past decade, to appreciate the limits of their authority. A peace officer undoubtedly has lawful power in an emergency, or when a crime is being committed or is about to be committed, to take reasonable steps to protect the lives of persons or to apprehend offenders. But this power ought not to be invoked by a well-trained policeman in other situations where the possibility of violence is general rather than immediate.

B. R.C.M.P. POLICIES AND PRACTICES

8. Security Service countermeasures were developed over the years sometimes on the initiative of Headquarters and sometimes as a result of local initiatives. Any countermeasures that could be called a 'programme' would require the support and even the initiative of Headquarters because of the need to commit resources of money and personnel to such activity. The current "policy", as stated on July 4, 1977, by the then Deputy Director General (Operations),

Assistant Commissioner Sexsmith, requires all countermeasures operations to be approved by the Deputy Director General (Operations) and to be "conducted within the limits of lawful authority and by legal means". However, there is evidence that the requirement of approval by the Deputy Director General (Ops) is not regarded as more than a general rule, and that countermeasures approved by the officer in charge of a 'desk' or section at Headquarters will not be regarded as unauthorized.

9. Within the R.C.M.P., both in the Security Service and in senior ranks of the R.C.M.P. generally, many forms of countermeasures have been well-known for decades. Perfectly proper methods of countering include: encouraging foreign intelligence officers to become double agents or to defect; briefings of government departmental officials or travellers as to the dangers of compromise; lawful arrest and prosecution. At the other extreme are disruptive tactics that include an element of unlawfulness, such as some of the CHECKMATE operations. While it is true that in the early 1970s the R.C.M.P. was urged to be "pro-active" — a word that appears to have been invented to describe action before the event rather than afterward — that word carries no connotation of illegality or indeed of anything more than the vigorous collection of intelligence before a crisis develops. Between these acceptable and unacceptable extremes are countermeasures that, while lawful in concept and execution, are in our view inappropriate functions of a security intelligence agency. Some examples of such countermeasures are inducing employers to discharge subversive employees, or leaking information to the media about the subversive characteristics of individuals, or undertaking "conspicuous surveillance" of domestic groups or attempting to prevent one group from subverting another political party.

C. EXTENT AND PREVALENCE OF COUNTERING MEASURES

10. Our analysis of 'extent and prevalence' applies not only to those countering measures that might be said to be "not authorized or provided for by law", but also to activities which, although they may have been lawful, are not acceptable. We analyze two categories of countermeasures — those carried out by some members of "G" Section of the Security Service, concerned with terrorism in Quebec, working in and outside Montreal in the early 1970s, and those carried out by members of the Security Service in several other provinces in the years 1971 to 1974 under the umbrella code names of ODDBALL and CHECKMATE.

11. The activities in Quebec included the following:

(a) The burning of a barn in which a meeting of a group believed to be subversive was to have been held. The evidence before us is that the object of the operation was to cause the group to move to another location where electronic surveillance would be feasible. However we cannot dispel from our minds the possibility that the members of the Security Service who participated in that incident also contemplated that the result would be a 'disruption' of the group's activities. There is no evidence to indicate that there was any other incident involving similar destruction of private property other than documents.

(b) Attempts in 1971 and 1972 to recruit human sources in groups believed to be violence-prone. To some extent disruption was the rationale behind the attempts. If in a particular case the attempt to recruit were to be successful, the result would be receipt of information about the activities of the group; if the attempt were unsuccessful, the attempt itself might become known to other members of the group who might then regard the target of the attempt with suspicion. Thus the very attempt might produce factionalism and disruption.

(c) Issuing a communiqué with the intention that the news media and members of the F.L.Q. and their sympathisers would regard it as a legitimate call to arms. There is no evidence that such a document was produced more than once by the R.C.M.P.

(d) Attempting to disrupt, by conspicuous surveillance, a meeting of members of an activist cell held in rural Quebec in September 1978.

12. The activities in other provinces, under the code names ODDBALL or CHECKMATE, were developed by a Special Operations Group at Headquarters. Members of the Security Service across Canada were encouraged to propose plans for new methods to help deal with threats of violence and of activities by political groups and organizations considered to be agents of hostile foreign powers. The evidence of those operations that were carried out included several that involved activities that might be characterized as "not authorized or provided for by law" in the sense that criminal acts may have been committed (attempting to render a vehicle inoperative, filing an income tax return in the name of another person, theft of a letter, and threats by phone). There was also one operation in which a criminal act (assault) was under consideration but not carried out. In our investigation of the nature, extent and prevalence, of these operations, the destruction of CHECKMATE files has made us entirely dependent on a few members of the Security Service, who have reconstructed what occurred from memory.

13. In addition, the following incidents have occurred. They may not have been unlawful in the circumstances, but represented activities the acceptability of which is a matter of policy. They will be discussed in Part V, Chapter 6. Some of these incidents occurred under Operation CHECKMATE; others did not:

(a) An approach to the employer of a person regarded as a terrorist or a supporter of a terrorist or a 'subversive' group with a view to persuading the employer to discharge the person. One incident is known.

(b) Dissemination of adverse information through the media, believed to be true, about an individual or group regarded by the Security Service as a security threat. Two incidents are known.

(c) Spreading information, believed to be true, designed to discredit the leader or other members of political or other organizations or to create dissension among 'subversive' groups. Two occasions are known.

(d) Spreading information, known to be false, designed to discredit a leader of an organization regarded as 'subversive'. One incident is known.

(e) Communicating anonymously with leaders of a political party to warn them that some members of their party were planning to attempt to obtain

delegates' credentials for the leadership convention of another political party in the hope of influencing the outcome of the convention. One instance is known.

D. LEGAL AND POLICY ISSUES

14. The present mandate of the Security Service authorizes it to "deter, prevent and counter" certain specified activities. Within the Security Service there has been no suggestion that these verbs should be assigned different meanings, and we can see no advantage in seeking to do so. Nor did the formal submission to the Cabinet in March 1975 discuss the meaning or consequences of these verbs.

15. Mr. Starnes and Mr. Dare consider that the use of these words in the Cabinet Directive of March, 1975, was in effect a declaration of already existing functions of the Security Service. Thus Mr. Starnes, both when he was Director General and when he testified before us on this subject in 1979, considered it natural that the Security Service should undertake a programme of countermeasures; he considered that the 'countering' work of a security intelligence agency is implied by the very use of the terms 'counter-espionage' and 'counter-subversion'.

16. Thus may words become masters. Whether or not the professional terminology authorized 'countering', two real questions remain: was, and is, 'countering' a proper and acceptable function of a security intelligence agency? If it is, what kinds of 'countering' are permissible and subject to what controls?

17. Some activities that may be characterized as "countering" are an inevitable and proper result of the work of such an agency. The collection of information, and its assessment and transformation into intelligence, may be said to be part of the countering process, in the sense that without collection and assessment nothing can be done, although to describe collection and assessment as countering is to expand the definition of the term beyond its real limits. A more obvious countering activity involves the 'turning' of a member of a hostile intelligence agency so that, while pretending to be still a genuine agent of that agency, he in fact provides information to the Canadian security intelligence agency. He becomes a double agent. If the Canadian agency can obtain such information about the activities of the hostile agency's espionage in Canada, those activities can be neutralized effectively. Thus the development of an 'agent in place' has 'countering' consequences, but it is unhelpful to describe this technique as a method of 'countering'. In reality it is providing a source of information that may also be used as a vehicle for a countering operation. It is not only legitimate but desirable for a security intelligence agency to be successful in persuading members of hostile foreign agencies to defect so that the Canadian agency and its allies will have an improved knowledge and understanding of the structure, personnel and methods of the foreign agency.

18. Information collected by the security intelligence agency is often transmitted to police forces and government departments, and may prompt these

authorities to take preventive measures against individuals or groups. For instance, security intelligence about terrorists is given to the police who are responsible for protecting international visitors, and intelligence about terrorist or espionage agents may be given to a police force having jurisdiction to investigate crime so that it can be used as evidence. Information about the secret intelligence activity of a foreign diplomat might be given to the Department of External Affairs so that the Secretary of State for External Affairs may decide whether to declare that diplomat to be *persona non grata* or otherwise let it be known to the foreign country that his activities are unacceptable. Similarly, in the security screening process, reports from the security intelligence agency will affect decisions by government departments to deny security clearance. The security intelligence agency may also pass information directly to individuals in preventive security briefings. For instance, the agency may warn Canadians posted abroad or intending to travel in certain countries of the methods which may be used to induce them to become sources for a foreign agency. In all of the foregoing situations, the preventing or countering action is taken by a police force or government department exercising an authorized governmental function, and the security intelligence agency's contribution is confined to its proper role of collecting and reporting security intelligence.

19. In the past, the "deterring preventing and countering" role of the R.C.M.P. Security Service went far beyond the proper functions of a security intelligence agency. Countering activities that are not acceptable include any that are contrary to the law of Canada, whether it is a federal, provincial or municipal law or the common law or the Quebec Civil Code. The legal issues arising from any of the incidents mentioned earlier which may have involved acts "not authorized or provided for by law" are analyzed in a separate Report. As we have noted, the legality of Security Service countermeasures was not a consideration for R.C.M.P. officers. This disregard for the rule of law is completely unacceptable under the system which, later in this Report, we shall propose for the future. No countermeasure should have been permitted which violated any Canadian law. No unlawful countermeasures by the security intelligence agency should be permitted in the future. Nor do we see any need to recommend changes in the law which would make otherwise unlawful countering measures lawful.

20. There are also countermeasures designed to disrupt the activities of groups or of individuals regarded as subversive which, while not unlawful, are nevertheless objectionable and unacceptable. This is particularly the case when the individuals concerned are Canadians employed in purely domestic political activities and not acting as foreign agents. We find it entirely inappropriate for the Canadian state, through an agency the operations of which are essentially secret, to take coercive measures against Canadian citizens and put them at a serious disadvantage. Later in this Report, in Part V, when we set out our recommendations on the laws and policies which should govern the Government of Canada's security intelligence activities, we shall discuss in detail the kinds of countering activity which must be avoided in the future as well as those which are acceptable.

21. The Security Service's use of unlawful countermeasures and those unacceptable measures referred to in the last paragraph was a grave mistake. These methods violated the rule of law, inflicted damage on Canadian citizens and involved secret attempts to manipulate political events and the news media. Such practices not only violate important precepts of Canadian democracy but they may also seriously damage the security agency itself. First there is the corrupting effect which the carrying out of such 'dirty tricks' is likely to have on the ethos of the security intelligence organization. Secondly, there is the loss of public respect which the disclosure of such tactics is likely to engender. Approval of such tactics will reduce the public's support for any kind of secret security intelligence activities.

CHAPTER 8

PHYSICAL SURVEILLANCE

A. ORIGIN, NATURE AND PURPOSE OF THE PRACTICE

1. When it is used in the course of R.C.M.P. investigations, the term "physical surveillance" includes the following practices:

(a) the use of static or mobile facilities to observe activities occurring in and around a fixed target such as a building;

(b) the use of cars, motorcycles, airplanes or boats to follow a target;

(c) the deployment of persons on foot to follow and watch a target; and,

(d) the use of technical aids to surveillance.

While the purpose of physical surveillance has remained unchanged, techniques have grown more complex over the years to cope with increasingly sophisticated methods of transportation and counter-surveillance. In the Security Service, physical surveillance is used to monitor the clandestine activities of intelligence agents from hostile countries, domestic groups which pose a threat to Canada's security, and agents of international terrorism. This surveillance enables the Security Service to acquaint itself with the personal habits of the human targets, follow their movements, and learn of any clandestine relationships they may be cultivating in this country.

2. Physical surveillance operations on the criminal side, unlike those in the Security Service, are usually aimed at obtaining information which will result in a criminal prosecution. It is for this reason that C.I.B. surveillance operations are generally of shorter duration than their Security Service counterparts. Physical surveillance by the C.I.B. is frequently directed at drug crimes and organized criminal activities.

3. Because of their different organization and objectives, it is convenient to deal separately with the structure of the Security Service and C.I.B. surveillance units.

The Security Service

4. One branch of the Security Service is responsible for visual monitoring on behalf of all the main operational branches of the Service. It is basically a technical service unit called in to provide visual surveillance of targets in counter-espionage or counter-subversion operations, and is often referred to as the "Watcher Service". Although its responsibilities were later expanded to

provide surveillance support for all Security Service activities, initially it was created to satisfy the surveillance needs of the Counter-espionage Branch and in fact was first a section of that Branch.

5. The creation of the Watcher Service was inspired by considerable clandestine espionage activity on the part of Communist bloc intelligence services, a significant portion of which was going undetected. A greater commitment to physical surveillance was intended to uncover that activity. The part-time surveillance effort in use until 1954 was incapable of meeting the challenge posed by increased foreign activity in Canada. The Security Service committed itself to the creation of a surveillance operation intended to possess a high level of skill and continuity of experience. In essence, the Security Service sought to specialize.

6. Surveillance, when required, may also be handled by regular members, most of whom have received training from Watcher Service members, as have many C.I.B. members and officers from other police forces.

The Criminal Investigation Branch (C.I.B.)

7. Before the early 1970s, surveillance of a criminal target was carried out according to manpower and equipment availability, without central co-ordination by a particular branch. No specialized group capable of conducting intensive coverage existed. Results of surveillance were haphazard. In the early 1970s, investigators at Montreal's "C" Division were conducting wide-ranging surveillance of targets. Because these targets routinely employed counter-surveillance methods, a need was recognized for a specialized surveillance unit, capable of maintaining surveillance on difficult targets. This gave rise to the first specialized C.I.B. surveillance team, which responded to requests for surveillance on targets of interest to various C.I.B. sections at "C" Division. Subsequently, specialized surveillance teams were introduced to several other divisions.

8. In March 1973 the R.C.M.P. designated the National Crime Intelligence Branch (N.C.I.B.) to co-ordinate policy and supervise the activity of surveillance sections in C.I.B. divisions throughout Canada. In July 1974 the N.C.I.B. surveillance sections were renamed Special "O" Sections. Terms of reference now govern the duties and operational procedures for Special "O" Sections. The duties include the collection of strategic and tactical criminal intelligence on predetermined targets, familiarization through surveillance with the habits and descriptions of regional organized crime figures, obtaining photographs of suspect individuals, buildings and meetings, and reporting random sightings of organized crime figures. In addition, surveillance assistance is given to all R.C.M.P. investigative squads and other Division Criminal Intelligence Service (D.C.I.S.) sections. Special "O" Sections are comprised of regular members, who fill most of the supervisory positions, and Special Constables who comprise the surveillance teams. Special Constables are given preparatory training for eight weeks. As in the Security Service, C.I.B. surveillance units have been forced to employ increasingly sophisticated techniques as targets themselves become more adept at detecting and countering surveillance.

B. LEGAL ISSUES

9. There are three categories of statutes which have presented difficulties for surveillance work:

— those governing "rules of the road";

— those governing the identification of persons and property; and

— those relating to trespass.

Rules of the road

10. The movement of motor vehicles on the highway is primarily regulated by provincial statute. Representations made to us indicate that adhering to these rules of the road when engaging in intensive surveillance operations has not always been possible. Indeed, Watcher Service training has emphasized that "there is no place for timidity in surveillance work". One result of this lack of timidity has been the violation of provincial traffic laws — particularly when a vehicle carrying the target might itself not comply with traffic laws. In addition to the violation of provincial laws, surveillance team members may have breached municipal by-laws by committing "non-moving" violations.

11. We have examined instances where surveillance was unsuccessful because traffic laws were obeyed and we are satisfied that compliance with present traffic laws must in many cases be responsible for the loss of surveillance and a consequent loss of effectiveness of the security operation.

12. The following provincial traffic violations have been specifically brought to our attention: speeding, proceeding the wrong way in one-way traffic, illegal U-turns and failure to stop. The list of possible violations includes:

— unnecessarily slow driving

— failure to yield right of way

— improper turns or signals

— failure to obey traffic lights

— failure to drive in proper lane

— improperly overtaking other vehicles

— following too closely

— failure to yield for emergency vehicles

— failure to stop at railway signals

— failure to obey instructions posted on traffic signs.

Municipal "non-moving" violations have also occurred when surveillance drivers have stopped in a no-stopping or loading zone in order to maintain observation of a target.

13. The Criminal Code also creates offences in relation to the operation of motor vehicles on the roadway. Section 233(4) affords an example:

> (4) Every one who drives a motor vehicle on a street, road, highway or other public place in a manner that is dangerous to the public, having regard to all the circumstances including the nature, condition and use of

such place and the amount of traffic that at the time is or might reasonably be expected to be on such place, is guilty of

(a) an indictable offence and is liable to imprisonment for two years, or

(b) an offence punishable on summary conviction.

There has been no evidence before us to suggest that Criminal Code offences (such as criminal negligence and dangerous driving) relating to the operation of motor vehicles have been committed by those engaged in physical surveillance in order for them to carry out their duties. Nor has there been any suggestion that any authority to drive in such a manner is necessary in the future.

The most recent attempt by the R.C.M.P. to state policy in regard to traffic laws

14. A "bulletin" from the Commissioner of the R.C.M.P., Bulletin OM-82, sent to all members of the Force (both C.I.B. and the Security Service) on August 25, 1980, states:

> Every member of the R.C.M.P. discharging covert surveillance responsibilities, or overtly responding to emergencies is expected to comply with all relevant provincial statutes, regulations and municipal by-laws.

The bulletin then promulgates "guidelines" to apply in "exceptional" circumstances, where "total" or "strict" compliance with "provincial statutes, regulations and municipal by-laws relating to traffic control" may, "because of the nature and seriousness of an investigation", not be "necessary in the public interest".

15. The guidelines are as follows:

> (i) Legal authorities and various provincial and federal statutory enactments provide certain legal protection to members of the R.C.M.P. when acting reasonably and responsibly in the discharge of those duties they are empowered to perform.
>
> (ii) Notwithstanding that certain legal protection would be provided to members of the R.C.M.P. reasonably conducting their surveillance and pursuit duties, every member is expected to comply with provincial and municipal motor traffic requirements unless:
>
> — to do so would seriously inhibit and prevent surveillance and/or pursuit activity; and
>
> — there are exceptional circumstances; and
>
> — when;
>
> A. There are reasonable and probable grounds to believe,
>
> (1) Life is in danger;
>
> (2) An indictable offence is in progress;
>
> (3) An indictable offence is about to be committed;
>
> (4) An indictable offence has been committed, is under active investigation, and the surveillance and/or pursuit is essential for purposes

of either identifying those responsible for that specific offence, or collecting evidence deemed necessary for prosecution, or

B. The surveillance or pursuit is in regard to:

(1) Persons known to be currently active in major criminal activity, when it becomes apparent that crimes are being planned, the exact nature and extent of which are still undetermined.

(2) A V.I.P. visit where it is necessary to keep surveillance on or to pursue persons who might cause harm or serious disruption, and the surveillance or pursuit is taking place during the course of that visit, not in preparation therefor.

(3) The protection of Government property, as in the case of maintaining discreet surveillance on the carrier of a flash roll during undercover operations.

(4) Investigations with respect to subversive activity as defined in the Official Secrets Act.

Thus the Commissioner has told members engaged in surveillance duties that, apart from cases where the law *might* afford a defence (such as the defence of necessity) to a charge — for instance of going through a red light or speeding — members may ignore such laws if the conditions in the guidelines are all satisfied.

16. The "bulletin" is stated on its face to be part of the Operational Manual of the Force and the Commissioner has confirmed to us that it forms part of that Manual. The bulletin states that "The following general guidelines *must* therefore be adhered to in the future". (Our emphasis.) If those words constitute an "instruction or order", then failure to comply with them would be a breach of the Commissioner's Standing Order I.4.C.1.a. which reads:

> The conduct and activities of a member shall at all times be such as to bring credit to himself and to the Force. A member shall not:
>
> Contravene or fail to comply with any oral or written instruction or order issued in a manner authorized by the Commissioner.

Breach of such a standing order is a minor service offence under section 25 of the R.C.M.P. Act. However, the Commissioner has advised us that, notwithstanding his use of the imperative word "must" in the bulletin, he did not intend the bulletin to be an "order". He says it is "only a guideline". In our opinion it would be difficult for a member receiving the bulletin to know the legal nature of it. At the very least the member would be likely to regard the bulletin as advice from the Commissioner that conduct which, in the case of an ordinary citizen or even a policeman "cruising" in a patrol car would be a violation of provincial or municipal traffic laws, will be permitted by the Force in the sense that no disciplinary action will result if a member engages in the same conduct in the circumstances described in the bulletin. The Commissioner has told us that what he intended to convey by the bulletin may be summarized as follows:

(a) as a general principle every member of the R.C.M.P. engaged in surveillance activities is expected to comply with all provincial statutes and regulations and municipal bylaws;

(b) where certain conditions are met, activities which otherwise would be violations of those statutes, regulations or bylaws do not constitute such violations;

(c) the reference to "legal authorities and various provincial and federal statutory enactments..." providing legal protection to members is to such matters as the protection afforded by section 25 of the Criminal Code, section 26 of the Interpretation Act, defences such as that contained in the New Brunswick Police Act and common law defences such as necessity or the immunity alleged to exist for members of the R.C.M.P. as agents of the Crown;

(d) in essence, the bulletin sets out circumstances in which, according to the R.C.M.P.'s interpretation of various statutory and common law defences and immunities, no violations of provincial laws and regulations or municipal bylaws occur.

In promulgating this bulletin the Commissioner relied in part on legal advice obtained from the Department of Justice. In Part IV we discuss the various "defences", such as the common law defence of necessity, the "implied powers" provision of section 26.2 of the Interpretation Act, the "justification" principle embodied in section 25.1 of the Criminal Code, and the various doctrines of immunity, and we intend in the ensuing paragraphs to review each of these briefly in the present context. In addition, as far as New Brunswick is concerned, there is a provincial statutory defence to provincial offences; this defence is referred to by us in Part V, Chapter 4. In the following brief comments which we make with respect to the Commissioner's bulletin, what we say is fully applicable only to those provinces which do not have a statutory defence, i.e. all provinces other than New Brunswick.

17. The common law defence of necessity would be available in regard to provincial offences.[1] It would likely be available if life is in danger, or if an indictable offence is in progress or is about to be committed or has been committed and there is "hot pursuit" of the culprit, but even then it would be necessary to balance the competing interests identified in *Morgentaler* v. *The Queen*, which we discuss in Part IV. Focussing our attention on the specific situations referred to in Bulletin OM-82, we do not think that the defence of necessity would be available if "an indictable offence is in progress, or is about to be committed or has been committed and the surveillance or pursuit of the culprit is essential for the purposes of either identifying those responsible for that specific offence or collecting evidence deemed necessary for prosecution". For example, a member driving a police vehicle while engaged in attempting to identify a thief or a person who has wilfully damaged property, or attempting to collect evidence of such offences, would not be able to rely on the defence of necessity if he were charged with speeding or failing to stop at a stop sign or a

[1] As a matter of principle, the common law defence of necessity would be available for provincial offences, at least to the same extent as in prosecutions under the Criminal Code. See *R.* v. *Walker* (1979) 48 C.C.C. (2d) 126 at 144 (Ont. Co. Ct.). In Ontario now the provision found in section 7(3) of the Criminal Code, which preserves common law defences, is copied in respect to provincial offences: the Provincial Offences Act, 1979, ch. 4, section 80.

red light. Similarly, we do not believe that the defence of necessity would be available where traffic violations are committed by a member conducting surveillance of those planning indictable offences, suspected of intending harm to visiting V.I.P.s, or plotting damage to government property. The sense of proportion between the perceived harm in the conduct of the criminal and the departure from regulated conduct on the part of the member — so essential to the application of the defence — cannot be assumed in advance as the Bulletin seems to do.

18. In Part IV we also discuss section 26(2) of the Interpretation Act and express the opinion that it cannot be invoked as authority in support of an implied power to do that which otherwise would be unlawful. We also discuss section 25(1) of the Code and, citing *Eccles* v. *Bourque*, conclude that it provides justification for a peace officer only for the use of "force" and then only when the law requires or authorizes him to do the very thing in question; violating a traffic law would probably fail to satisfy either condition in a number of the circumstances specifically referred to in the Bulletin.

19. It is apparent from what we have learned that the Commissioner's Bulletin is also founded on advice that provincial law is not applicable to actions of members of the R.C.M.P. that are "reasonably necessary to enable them in particular circumstances to carry out duties and responsibilities assigned to them by or under federal legislation". This opinion is founded on the statement by Mr. Justice Pigeon, delivering the reasons for judgment of the Supreme Court of Canada in the *Keable* case,[2] that the R.C.M.P. is a branch of the Department of the Solicitor General and its management as part of the Government of Canada is unquestioned. The advice given to the R.C.M.P. appears to be an invocation of certain of the doctrines of immunity which we discuss fully in Part IV. We consider that, in its stated breadth of application, it is likely not an accurate statement of the law, and that it may be an invalid foundation for the Commissioner's Bulletin. We emphasize that we do not criticize Commissioner Simmonds, who is entitled to rely on such advice, especially when it comes from the source from which it did come. Consequently, we have serious doubts as to the legal foundation of Bulletin OM-82. We realize that it is not easy to frame guidelines for members concerning these matters, in the light of the present state of the law. Implementation of our recommendations would result in both the R.C.M.P. and the security intelligence agency having less difficulty in instructing their members in the future. In the meantime, for the reasons we shall give in Part IV, we do not think that members of the R.C.M.P. should rely on Bulletin OM-82 as authority which could be cited as a defence if they are faced with charges under provincial or municipal traffic laws, except in those circumstances when the defence of necessity would properly apply.

Laws governing the identification of persons and property

20. A number of federal and provincial statutes require the accurate identification of persons or property. Examples include various provincial enactments

[2] *Attorney General of Canada* v. *Keable* [1979] 1 S.C.R. 218 at 242.

requiring hotel guests to register in their proper names, and highway traffic legislation requiring individuals to hold a valid driver's licence and identify their automobiles with provincially issued licence plates.

21. Registration and identification requirements are incompatible with the covert nature of surveillance operations. As in the case of undercover operations involving members or human sources, the ability to conceal one's true identity successfully is essential in physical surveillance operations. A target, once aware of a surveillance effort, may simply delay his intended clandestine or criminal activity, or deliberately mislead the surveillance team. Furthermore, the team, once "burned" (exposed to a target) is of little value in further covert surveillance of that target. Hence, the need has arisen for surveillance cars to have licence plates that cannot be traced to the R.C.M.P., and for members to hold identification documents that allow them to remain in proximity to a target without disclosing their true identity.

22. At present, the two most commonly used false identification documents are drivers licences and vehicle registrations. This documentation has in the past been obtained in a number of ways: applying for the document in the normal manner, but supplying false information in the application; entering into agreements with senior departmental officials for the issuance of documents and, manufacturing high quality false documentation by the R.C.M.P.

23. Supplying a false statement in an application for a driver's licence (in order to obtain a licence in a false name) is an offence in most provinces, as is the possession or use of a fictitious licence. Further violations occur in some provinces where an individual holds more than one valid licence or applies for a second licence while holding a valid licence. Finally, a licence may be invalid in some provinces unless signed in the "usual signature" of the individual licenced.

24. Dual registration of a surveillance vehicle violates other Highway Traffic Act provisions in a number of provinces. Over the years a variety of practices have been used to disguise the ownership of R.C.M.P. surveillance vehicles. It is impossible to outline every variation of this practice; a few examples, however, are illustrative. In some cases, a car owned by the R.C.M.P. was registered in the name of an "ostensible owner", who may have falsely indicated in an application for registration that he was the true owner. In other cases, an additional set of plates may have been obtained through making an application, with the co-operation of provincial Registrars of Motor Vehicles, for vehicles already registered in the name of the R.C.M.P. It is an offence under provincial Highway Traffic legislation to make false statements (e.g. as to the applicant's true identity, or the ownership of a vehicle) in an application for registration; it is also an offence in some provinces to use licence plates other than those registered or issued for a vehicle. Finally, the use of out-of-province licence plates after a defined period of time may violate Highway Traffic legislation.

25. Where a licence or registration has been obtained through making a false statement in an application, such a statement may amount to a false pretence

under section 320 of the Criminal Code. Section 319 defines a false pretence as follows:

> (1) A false pretence is a representation of a matter of fact either present or past, made by words or otherwise, that is known by the person who makes it to be false and that is made with a fraudulent intent to induce the person to whom it is made to act upon it.

26. Section 320 states:

> (1) Every one commits an offence who
>
> (a) by a false pretence, whether directly or through the medium of a contract obtained by a false pretence, obtains anything in respect of which the offence of theft may be committed or causes it to be delivered to another person;
>
> (2) Every one who commits an offence under paragraph (1)(a)
>
> (a) is guilty of an indictable offence and is liable to imprisonment for ten years, where the property obtained is a testamentary instrument or where the value of what is obtained exceeds two hundred dollars; or
>
> (b) is guilty
>
> (i) of an indictable offence and is liable to imprisonment for two years, or
>
> (ii) of an offence punishable on summary conviction,
>
> where the value of what is obtained does not exceed two hundred dollars.

On some occasions false registration and identification documents have been manufactured by the R.C.M.P. for use by the Criminal Investigations Branch in lieu of having members apply for licences and other forms of documentation. The manufacture of these documents may have amounted to forgery under section 324 of the Criminal Code. That section reads, in part:

> 324. (1) Every one commits forgery who makes a false document, knowing it to be false, with intent
>
> (a) that it should in any way be used or acted upon as genuine, to the prejudice of any one whether within Canada or not, or
>
> (b) that some person should be induced, by the belief that it is genuine, to do or to refrain from doing anything, whether within Canada or not.
>
> (3) Forgery is complete as soon as a document is made with the knowledge and intent referred to in subsection (1), notwithstanding that the person who makes it does not intend that any particular person should use or act upon it as genuine or be induced, by the belief that it is genuine, to do or refrain from doing anything.
>
> (4) Forgery is complete notwithstanding that the false document is incomplete or does not purport to be a document that is binding in law, if it is such as to indicate that it was intended to be acted upon as genuine.

27. Section 326 of the Code creates an offence when the forged document is used:

> 326. (1) Every one who, knowing that a document is forged,
>
> (a) uses, deals with, or acts upon it, or

(b) causes or attempts to cause any person to use, deal with, or act upon it,

as if the document were genuine, is guilty of an indictable offence and is liable to imprisonment for fourteen years.

28. When a member engaged in surveillance assumes the identity of a person, whether living or dead, he may violate section 361 of the Criminal Code. That section reads:

> Every one who fraudulently personates any person, living or dead,
>
> (a) with intent to gain advantage for himself or another person,
>
> . . . or
>
> (c) with intent to cause disadvantage to the person whom he personates or another person,
>
> is guilty of an indictable offence and is liable to imprisonment for fourteen years.

In most surveillance operations there is no personation of a person "living or dead", so that no offence is committed. Where, however, an individual engaged in surveillance might purport (although we have seen no examples) to be another person, living or dead, he may violate the section.

29. In order for the offence to occur, the personation must also be fraudulent and the personator must intend to gain advantage for himself or cause disadvantage to the person he personates or another person. The word "advantage" in section 361 has been afforded a broad interpretation. In *Rozon* v. *The Queen*[3] Mr. Justice Montgomery stated:

> The words "gain advantage" could scarcely be more general in their scope, and I find nothing to suggest that their application should be restricted to an advantage appreciable in money.[4]

Mr. Justice Crête held that the word "advantage" must be taken in its larger meaning. [Our translation]

> In reading this text, one can see that the legislator has declared guilty of an indictable offence anyone who personates someone (a) to gain advantage — without specifying its nature; (b) to obtain any property or an interest in a property — this is specific, in view of the definition of the word "property" given in section 2 of the Criminal Code; (c) to cause disadvantage to another person — here again, without specifying the nature of the disadvantage.[5] [Our translation]

This reasoning was accepted in Ontario in *Regina* v. *Marsh*.[6] Thus it appears that almost any advantage or disadvantage is encompassed by section 361. Nonetheless, it may still be questioned whether the courts, in construing "advantage" so broadly, intended it to encompass the *investigative* advantage gained through personating another individual.

---

[3] (1974), 28 C.R.N.S. 232 (Quebec C.A.).

[4] *Ibid.*, at p. 233.

[5] *Ibid.*, at p. 237.

[6] (1975) 31 C.R.N.S. 232 (Ont. Co. Ct.).

30. The most significant restriction in section 361 is the requirement that the personation be "fraudulent". In *Rozon* v. *The Queen*, Mr. Justice Crête adopted a narrow construction of the word:

> In my opinion, the word fraudulently as used in section 361 is an adverb of manner which involves bad faith as opposed to good faith, or to an honest error.[7] [Our translation]

It therefore appears that an individual engaged in surveillance who personates another person, living or dead, and gains an advantage or causes a disadvantage thereby within the meaning of section 361, nonetheless commits no offence as long as he does not act in bad faith. The section then appears likely to be of no consequence in relation to surveillance operations which are carried out in good faith, i.e. for purposes falling within the mandate of the Security Service or the policing duties of the C.I.B.

31. The interpretation of section 362 of the Criminal Code, however, is problematical. That section, dealing with personation at an examination, reads as follows:

> 362. Every one who falsely, with intent to gain advantage for himself or some other person, personates a candidate at a competitive or qualifying examination held under the authority of law or in connection with a university, college or school or who knowingly avails himself of the results of such personation is guilty of an offence punishable on summary conviction.

We are aware of at least one instance, although not a surveillance operation, where this section may have been violated. As we have seen in our examination of section 361, the word "fraudulently" in that section implies bad faith on the part of the personator; the word "falsely" in section 362 may be interpreted in a similar fashion, thus absolving a personator acting in good faith (e.g. in order to carry out the mandate of the Security Service). The little case law which has construed the word "falsely" seems to support this interpretation. In *Rex* v. *Frank*,[8] Chief Justice Campbell of Prince Edward Island found that the offence of making a false statement in the Income War Tax Act, R.S.C. 1927, involved not merely an inaccurate statement, but one made fraudulently, with *mens rea* or intent to deceive. A number of American cases have reached similar conclusions.[9] Yet, "falsely" in section 362 is not so clearly defined that we can ignore the possibility that Security Service activities of the nature mentioned here violate the section. The example we have cited is not the only activity of this nature of questionable legality: individuals engaged in surveillance operations might also have violated section 362 if they chose to obtain their "cover" licences by supplying the name of a real person when taking their qualifying tests. We are not aware of any specific instances where individuals engaged in surveillance have personated other individuals in a manner that violates section 362; that does not mean, however, that the practice has not occurred. In any

---

[7] (1974) 28 C.R.N.S. 232 at p. 238 (Quebec C.A.).

[8] (1945) 84 C.C.C. 94 (P.E.I.S.C.).

[9] *U.S.* v. *Achtner*, 144 F. 2d 49 (C.C.A.N.Y.); *Fouts* v. *State*, 149 N.E. 551; *U.S.* v. *King*, 26 Fed. Cas. 787; *U.S.* v. *Otey* 31 F. 68.

event, this brief discussion serves to highlight the potential for running afoul of these sections as the R.C.M.P. search for new and legal means of obtaining "cover" documentation.

32. Disguising one's proper identity may also have resulted in violation of provincial hotel registration legislation. A number of provinces have legislation prohibiting hotel guests from registering in an assumed name or falsely stating their place of residence. This problem has been identified in four provinces in particular — Nova Scotia, Prince Edward Island, Ontario and British Columbia.

Laws relating to trespass

33. The surveillance sections of the Security Service and the C.I.B. have both indicated to us that violations of petty trespass legislation are inherent in surveillance operations. Common examples include entering parking garages in apartment buildings to determine the presence of a target's vehicle and entering an apartment building in order to determine by listening from a corridor whether the target is within an apartment. These activities may, depending on the circumstances, constitute a trespass to property in provinces having trespass legislation.[10] In addition, they may give rise to the Criminal Code offences of Mischief and Trespassing at Night.

34. Nova Scotia, Prince Edward Island and Saskatchewan have no trespass legislation. Trespass legislation in British Columbia and New Brunswick applies to narrow factual situations which are not relevant here, and the Quebec statute, the Agricultural Abuses Act, is probably restricted to agricultural lands. Petty trespass legislation in Alberta and Newfoundland requires notice not to trespass by word of mouth or in writing, or by posters or sign boards, before an offence is committed and so poses problems where such notice is given. Legislation in Ontario and Manitoba, however, does not in every case require such notice, and therefore poses the greatest difficulty for surveillance operations. In Ontario, an offence occurred until 1980 when there was unlawful entry upon enclosed land, a garden or lawn, or land on which the entrant has had notice not to trespass; under the new Act there is an offence when there is unauthorized entry onto premises "enclosed in a manner that indicates the occupier's intention to keep persons off the premises". In Manitoba, the offence in part consists of entering into any land or premises which is the property of another and is wholly enclosed.

35. In Chapter 2 of this part, the Criminal Code offence of trespassing at night (section 173) was discussed in relation to surreptitious entries. This offence is equally germane for those who, in the course of conducting surveillance of a house or an apartment at night, "loiter or prowl" near such buildings. If individuals engaged in surveillance merely enter a parking garage to determine the presence of a target's car, and then leave they likely cannot be said to be "loitering" in the sense of "hanging around".[11] Nonetheless, if they

---

[10] The statutes are referred to in Part III, Chapter 2, footnotes 20 to 26.

[11] *R.* v. *McLean* (1970) 1 C.C.C. (2d) 277; 75 W.W.R. 157 (Alta. Mag. Ct.).

enter the garage they may be "prowling", in the sense of "hunting in a stealthy manner for an opportunity to commit a criminal offence" (in this case, mischief, contrary to section 387).[12]

36. Where physical damage, even nominal, occurs to a target's vehicle in the course of an operation, section 387(1)(a) of the Criminal Code, dealing with the wilful damaging of property, may have been violated. In addition, an offence may have been committed under section 388(1) of the Code, dealing with the wilful destruction or damaging of property. It can also be argued that merely handling the vehicle of the target amounts to a trespass upon chattels and is thus an interference with the lawful use or enjoyment of the property contrary to section 387(1)(c). If this is so then the indictable offence of mischief has been committed. Quite apart from possible criminal implications, the tampering with a vehicle, even if it does not result in any damage to the vehicle, may be trespass at common law. The R.C.M.P. position, based on legal advice, is that there is a conflict of judicial authority as to whether trespass to a chattel (a thing) is actionable — i.e. is a wrong — without proof of damage. In our view there is not a conflict of judicial authority,[13] but an absence of judicial authority except for quotations of textwriters by judges. The textwriters quoted assert that in principle trespass to chattels should be no different from trespass to land. In regard to the latter the common law is clear that there may be trespass without damage.

Laws relating to violation of privacy

37. In British Columbia it has been held[14] that a private investigator had not violated the statutory guarantee of privacy by affixing a bumper beeper — a small radio transmitter emitting signals to enable the location of the vehicle to be traced — to the bumper of a car. The car belonged to a husband who was being watched by the investigator pursuant to instructions given by the wife. The court had regard to the fact that the wife was not motivated by malice or curiosity, that she had not attracted public attention, that she had not acted in an offensive manner and that her conduct was therefore reasonable. The use of a "bumper beeper" is probably not in violation of Article 5 of the Quebec Charter of Rights and Liberties of the Person, at least while the vehicle is travelling on public roads. However, it has been argued that attaching such a device to the personal effects or clothes of a person could be a violation. We express no view in that regard.

---

[12] *Ibid.*

[13] The R.C.M.P. position was based on three cases. One was said to support the view that trespass to a chattel is not actionable without proof of damage; but a reading of the case — *Everitt* v. *Martin* [1953] N.Z.L.R. 298 — indicates that the court there went no further than to cast doubt upon actionability without proof of damage. The other two cases cited were Canadian cases: *Demers* v. *Desrosiers* [1929] 2 W.W.R. 241 (S.C. of Alta.) and *Wolverine S.S. Co.* v. *Canadian Dredging* [1930] 4 D.L.R. 241 (S.C. of Ont.). In the first case the court did not decide the point but quoted three English textbooks which suggest that the law is or should be that trespass to chattels is actionable without proof of damage. In the second case the point was not decided.

[14] *Davis* v. *McArthur*, [1971] 2 W.W.R. 142 (B.C.C.A.).

Could surveillance constitute intimidation?

38. To this point we have not discussed the Criminal Code offence of intimidation (section 381). We have no documented instance where such conduct in physical surveillance operations has occurred in the past; therefore, the subject cannot properly be examined as a past practice not provided for or authorized by law. Nonetheless, we raise this offence as a legal issue, if only immediately to discount it, because of its apparent connection with physical surveillance activities in both the Security Service and the C.I.B. The relevant portions of section 381 read:

> 381. (1) Every one who, wrongfully and without lawful authority, for the purpose of compelling another person to abstain from doing anything that he has a lawful right to do, or to do anything that he has a lawful right to abstain from doing,
>
> (c) persistently follows that person about from place to place,
>
> ...
>
> (f) besets or watches the dwelling-house or place where that person resides, works, carries on business or happens to be,
>
> ...
>
> is guilty of an offence punishable on summary conviction.
>
> (2) A person who attends at or near or approaches a dwelling-house or place, for the purpose only of obtaining or communicating information, does not watch or beset within the meaning of this section.

39. Inherent in physical surveillance operations is the following (sometimes persistently) of individuals and observation around buildings, dwelling-houses, etc. It cannot be said, however, except perhaps in a few cases, that the persistent following or watching and besetting has been "for the purpose of compelling another person to abstain from doing anything that he has a lawful right to do, or to do anything that he has a lawful right to abstain from doing". In virtually every case, physical surveillance has involved no "compulsion"; rather it has involved discreet observation of a target. Second, in the few cases where the fact of surveillance has been deliberately made known to the target (for example, in order to frustrate an agent meet) and where therefore there may have been an element of compulsion, the activity in question was almost inevitably not one which the target had a lawful right to perform — the activity might have involved espionage or a criminal operation. Third, it probably cannot be said that surveillance teams, whether C.I.B. or Security Service, have acted "wrongfully" and "without lawful authority" in their pursuit of targets, at least insofar as they have acted in the discharge of their functions as peace officers in combatting crime and countering threats to security.

40. It is thus unlikely that section 381 has been violated by surveillance teams engaged in normal (covert) surveillance activities. The possibility of a violation does exist, however, where surveillance is carried out overtly, for example, in order to deter a domestic group perceived by the Security Service to be a threat to security. In such a case, there is intended to be an element of compulsion

resulting from the surveillance. If the group's activities are lawful, it may be that the Security Service would be acting "wrongfully" and "without lawful authority", thereby violating section 381.

R.C.M.P. attempts to inform provincial governments of legal problems associated with physical surveillance

41. Under this programme carried out early in 1978, the R.C.M.P. held briefing sessions with senior provincial officials in order to inform them of covert investigative techniques which may have contravened provincial statutes. In a letter dated June 6, 1978, Mr. Dare, Director General of the Security Service, reported the results of these briefings to the Solicitor General, the Honourable Jean-Jacques Blais. This letter stated:

> As a result of the Commissioner's instructions of 31 January 1978, the Security Service participated in a number of briefings to provincial Attorneys General on areas where the application of covert investigative techniques may have contravened provincial statutes. Specifically, the objectives, necessity and the consequences of discontinuance of i) alias documentation, ii) dual registration and the use of secret plates for motor vehicles, iii) registration in hotels or other accommodation using an alias.. . .

42. Briefings were carried out as follows:

Newfoundland	— February 3, 1978 — Deputy Minister of Justice briefed by C.I.B.
Nova Scotia	— February 2, 9, 1978 — Director General, Department of the Attorney General, briefed by C.I.B. and Security Service
New Brunswick	— May 11, 1978 — Deputy Minister of Justice and Director of Prosecutions briefed by C.I.B. and Security Service
Quebec	— February 7, 1978 — Deputy Attorney General, Assistant Deputy Minister — Criminal Prosecutions, Assistant Deputy Minister — Police Matters briefed by C.I.B. and Security Service
Ontario	— November 7, 1977 — Attorney General, Solicitor General and Assistant Deputy Attorney General briefed by C.I.B. and Security Service
	— January 11, 1978 — Assistant Deputy Attorney General briefed by C.I.B. and Security Service
Manitoba	— February 6, 1978 — Attorney General briefed by C.I.B. (after C.I.B. consultations with Security Service)
Alberta	— May 8, 1978 — Solicitor General briefed by C.I.B. and Security Service
British Columbia	— January 16, 1978 — Attorney General briefed by C.I.B.

— February 6, 1978 — Deputy Attorney General briefed by C.I.B.

(Note that some of the meetings took place before Commissioner Simmonds' directive of January 31, 1978).

43. There appears to have been no discussion with officials of the Saskatchewan Attorney General's department. Mr. Dare's letter to Mr. Blais explained that the Security Service in Saskatchewan carried out no covert operations which would contravene provincial statutes and that therefore the Attorney General would not be briefed.

44. There appears to have been no mention of possible violations of "rules of the road" under provincial highway traffic legislation or of possible violation of provincial petty trespass legislation during these briefings.

C. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

45. The initial policy issue is whether there is an established need for physical surveillance as an investigative tool for the Security Service and the C.I.B. If so, should changes be made in existing legislation in order to bring effective surveillance operations within the law? Should the changes give surveillance teams special powers so that they may lawfully drive in ways that in the case of other drivers would be offences under provincial or municipal laws? For example, if a member of the Watcher Service exceeds the posted speed limit in order to maintain surveillance of a target should the law be such that he is not guilty of speeding? If the answer is yes, and an accident ensues in which an innocent third party is injured, or his property is damaged, should that person be able to pursue a civil remedy by suing the individual member of the surveillance team, the R.C.M.P., or the federal or provincial governments? If not, should compensation be available through other means?

46. Many, although not all, of the statutes which have been violated during the course of physical surveillance operations might be referred to loosely as being "regulatory" in nature. To some observers, the violation of "regulatory" laws may seem to be unimportant. At least one newspaper commentator has said that breaches of "minor" laws by the R.C.M.P. is not a matter of concern. We disagree. In a national police force, or a security intelligence agency, the adoption of a policy that permits violations of "minor" laws is the thin edge of the wedge. If it is permissible to violate "minor" laws in the public interest (or more accurately, in what the members of the organization *decide* is in the public interest), then an attitude arises that makes it easier to tolerate violations of "major laws". An ethos is created that excuses what is done for noble reasons and asserts its validity. This cannot be acceptable.

47. At the same time, if we, as a democratic society, insist that the police and intelligence agencies, like all government institutions, must be subject to the law, we also wish to ensure that those agencies can perform their assigned tasks effectively. If "minor" laws will be obstacles to that effectiveness, and if a lawful exception to their application can be made *without damage* to the social

purposes of those laws, then the legislators should support amendments to those laws to attain that objective.

48. Physical surveillance operations are indispensable to both services of the R.C.M.P. Present laws pose obstacles for surveillance operations and result in unnecessary violations of the Rule of Law. Existing statutory and common law defences are inadequate. Legislation is needed to provide a statutory defence for individuals engaged in surveillance team operations, in defined circumstances, when their activities contravene some of the laws which restrict such operations at present. Where amendments are necessary in respect of provincial legislation (highway traffic, petty trespass laws etc.), such amendments should be enacted by the provinces concerned. Detailed recommendations are contained in Part V, Chapter 4 and Part X, Chapter 5.

CHAPTER 9

UNDERCOVER OPERATIVES

INTRODUCTION

1. In conducting both criminal and security intelligence investigations, the R.C.M.P. frequently gather information through persons who are not openly identified as members of the Force, or as persons working on its behalf. An undercover operative is often able to approach or infiltrate the subject of interest and so to obtain information which would not otherwise be accessible. The undercover operative may be either a member of the R.C.M.P. or an individual who has volunteered or been recruited by the Force. In the latter case, the individual may already be 'in place' near the target, or may be asked to approach it in his own or in a disguised identity and to gain acceptance.

2. The use of undercover operatives is at once one of the R.C.M.P.'s most effective investigative techniques and the one which causes the greatest difficulty and concern for the Force and the public at large: an undercover operative can gather more important information than any technical or mechanical source, but the nature of his task and the environment in which he must work often create considerable pressure on him to commit unlawful acts.

3. This chapter is devoted to an examination of the use by the R.C.M.P. of undercover operatives and the resulting practices and activities not authorized or provided for by law.

A. ORIGIN, NATURE AND PURPOSE OF THE PRACTICE

4. History abounds with tales of informers. That is true of the Canadian past as much as that of other countries. We described in Part II, Chapter 2, how, in the early days of Confederation, undercover operatives were used by the Dominion Police Force on both sides of the Canada-U.S. border to provide intelligence about the activities and intentions of the Fenians. The primary method of collecting information was to infiltrate informers into Fenian organizations. These undercover operatives often spent years within the organization, in some cases working their way into influential positions. From the early 1870s until the First World War, agents supervised by Commissioners of the Dominion Police continued to play a role in providing intelligence information about politically motivated violence in Canada. Although the North-West Mounted Police did not employ undercover operatives in dealing with the North-West Rebellion of 1885, they did so in policing the Yukon Territory

during the gold rush at the turn of the century. In investigating rumours of American plots to annex the Yukon Territory, the N.W.M.P. used operatives to infiltrate suspect organizations and groups.

5. During the First World War, both the Dominion Police Force and the Royal North-West Mounted Police used undercover operatives in domestic activities related to the war effort. Following the war, both agencies carried out extensive undercover operations to investigate the labour movement. In the years between the World Wars, the R.C.M.P. concentrated its intelligence activities on counter-subversion, frequently using its own members to infiltrate suspect organizations. The major targets of the Force in the late 1930s were Fascist and Nazi political organizations in Canada. One of the most celebrated instances of infiltration by Force members was that of Constable (later Superintendent) John Leopold. In 1921 Leopold managed to infiltrate the Communist Party in Canada. He remained undercover as a member of the Party until 1928, when his true identity was discovered and he was expelled. His testimony was later instrumental in securing the conviction of eight persons as members and officers of the Communist Party of Canada. Upon his subsequent transfer to Headquarters, Leopold began to work full time on the analysis of security files and reports coming in from the field. During the next two decades Leopold would be the R.C.M.P.'s number one resource person on Communism in Canada. He knew many of its leaders in Canada personally, was intimately acquainted with its activities and had a thorough knowledge of its ideology.

6. In criminal matters, individuals operating undercover were first used in earnest after the Second World War. They were deployed primarily in drug investigations, which are a continuing operational priority. The use of long-term undercover operatives for non-drug criminal investigations has never been extensive. The Criminal Investigation Branch has told us that it uses undercover operatives in non-drug investigations ". . . only where circumstances clearly indicate that it is necessary and after all potential results, favourable and otherwise, have been considered".

7. Those who work in an undercover capacity attract a variety of names which obscure the subtle categories into which they fall. Colloquially, undercover operatives are variously called spies, informants or secret agents. The Security Service itself uses the term "human sources" to describe civilian operatives, the more casual of whom are called "contacts".

8. For the sake of clarity we refer to members and non-members undercover as "undercover operatives", even though that expression is not used by the R.C.M.P. There is in fact no umbrella expression used by the R.C.M.P. to cover the various kinds of persons we refer to in this chapter. The general term it uses to describe all non-member operatives is "human sources". The categories into which undercover operatives fall are generally as follows:

(a) the volunteer source;

(b) the undeveloped casual source;

(c) the developed casual source; and

(d) the long-term, deep-cover operative.

While it is not possible to establish iron-clad definitions to cover every possible type of undercover operative, these are the leading distinctions.

The volunteer source

9. The volunteer source does not truly operate undercover. He may be an ordinary citizen who, overtly or otherwise, and often for a single occasion, approaches the R.C.M.P. with information relating to either a criminal or a security intelligence matter. No recruitment or active solicitation is involved, although the criminal investigation officers generally encourage responsible persons to come forward with information about crime, and the Security Service welcomes volunteered information from citizens and others about suspected espionage, subversion or terrorism. Volunteer sources may be motivated by more than good citizenship; they may be seeking favours in exchange for the information they will provide. A criminal may want protection from other criminals, or police intervention with prosecuting authorities in order to recommend a lighter sentence. On the security side, a foreign intelligence officer may furnish information in exchange for assurances of asylum and the provision of a new identity.

The undeveloped casual source

10. By way of contrast, what is called an "undeveloped casual source" may be attracted by solicitation. The approach is invariably low-key and falls short of an intensive "recruitment" but there is nonetheless a degree of active encouragement. Taxi drivers, maintenance or utility personnel, and hotel doormen are typical examples, since their normal tasks provide opportunities to observe targets. Such people are initially interviewed and their co-operation is sought. No reward or payment is offered. If they agree to help, discreet interviews are periodically arranged. Such sources play no covert role and do not disguise their identities by using false documents.

The developed casual source

11. The "developed casual source" differs from the undeveloped source in two respects: the nature of his recruitment and the frequency of contact with his 'handlers'. Before the first approach is made, the R.C.M.P. will assess his interests and decide upon an inducement most likely to attract his co-operation. Most frequently, casual sources recruited by the Security Service provide their assistance out of a sense of loyalty. Inducements may, however, be needed. If the source is a journalist, he could be offered preferred access to stories emanating from the Force. In criminal matters, money may be promised. For those awaiting sentencing, the Force may undertake to speak to the Crown Attorney about the prisoner's "co-operative attitude". The developed casual source will be more likely than his 'undeveloped' counterpart to be assigned an active information gathering role, rather than simply reporting what he sees or hears in the course of his usual activities. Although the source is described as a 'casual', his relationship with the Force may entail regular meetings and last for years. While his affiliation with the R.C.M.P. will be kept secret, his identity is not normally disguised, and he will not normally carry false papers.

The long-term deep-cover operative

12. By far the most intrusive undercover role is that of the long-term, deep-cover operative. Here, both members and human sources commit themselves to extensive, lengthy and often elaborate operations to infiltrate and remain inside a target's sphere. The ultimate long-term, deep-cover operative is the intelligence officer of a hostile foreign power who has been 'turned' by the Security Service into a 'double agent'. Because of the intensity, duration and danger of such operations, long-term, deep-cover operatives are usually paid for their intelligence, although some have worked for ideological reasons alone.

13. In determining whether the person deployed in an operation requiring a long-term, deep-cover operative will be a member or a human source, the R.C.M.P. considers such factors as an individual's ability to penetrate a given target, his trustworthiness, the extent of the control which will be required in handling the operative and the availability of members for the purpose. Since such a person will be committed to the role for periods sometimes as long as several years (and even, rarely, decades), the Force generally prefers to use sources and keep its members available for a greater variety of work.

14. Normally, only undercover members assume false identities for operational purposes. It is extremely rare for a source to use false identification documents during an operation, although such documents may be needed in order to protect him at a later stage from vindictive targets. For the most part, sources are chosen because of an existing personal history which allows them to approach a target without arousing suspicion. For example, the source might 'espouse' a philosophy similar to that of the target. The source used by the Security Service to penetrate the Western Guard (discussed below) was chosen on this basis.

15. Where members assume false identities for long-term, deep-cover work, they are provided with a fabricated life history, including such invented details as the names of schools and churches attended, former employment and previous addresses. These 'legends' are given credibility through identity cards, driver's licences and S.I.N. numbers which reflect the legend. No effort is spared to give every appearance of genuineness to the elaborately fabricated story, since some targets thoroughly investigate the personal histories given by prospective adherents; the consequences of detection could be grave. With his legend in place, the undercover member develops a cover story which gives the appearance of legitimacy to his approach to the target.

16. It is not uncommon that the long-term, deep-cover operative is compelled to dissociate himself for considerable periods from family and friends in order to perform his role. Such isolation, taken with the stress and danger often associated with undercover work, creates a need for able, dependable and firm handling by experienced members. A bond develops between the operative and his handler in such circumstances: a dependence arises which is virtually parental. The dynamics of the relationship must be anticipated and understood if control of the operative is to be maintained. Where control is lost, the operative is withdrawn.

17. Long-term, deep-cover operatives may require extensive training in the 'tradecraft' of spying. Theirs are the most sophisticated of operations, necessarily so because of the sophisticated nature of their targets, whether hostile intelligence agencies or organized criminal groups.

The use of undercover operatives

18. The general manner of using undercover operatives in the Security Service differs significantly from their use in criminal investigations. In the latter they are used mainly to obtain evidence for prosecutions, of which drug related charges form a significant part. Consequently, sources in criminal investigation work, like undercover members in such work, expect that their relationship with the R.C.M.P. will be exposed (or, in the vernacular of security and police work, that they will be 'burned') in a relatively short time — a matter of perhaps months, not likely more than a year. However, the Security Service seldom uses sources primarily for the collection of evidence for use in court; in the vast majority of cases the hope of the Security Service is that the source will provide information over a matter of at least months and frequently years without being 'burned'. One such case came to public attention with the testimony of Warren Hart before this Commission. Mr. Hart testified that he had been recruited by the R.C.M.P. from the United States and directed to infiltrate a radical Black movement in Canada. A false immigration record was arranged for him in order to enhance his credibility. Mr. Hart succeeded in penetrating the movement and related information to the R.C.M.P. while posing as a bodyguard for Roosevelt Douglas, one of the leaders of the movement.

19. If the source acquires information which is evidence of a crime, the Security Service may decide to lay charges, in which case it will do its utmost to preserve the 'cover' of the source by encouraging the police to obtain the same or other evidence by their own means. If that approach succeeds, the source will not have to testify and can thus continue to operate as a source in the same group or at least in the same milieu. The security intelligence agency's source will in any event not always acquire evidence of a crime. Even if he does acquire such evidence, for example, evidence of espionage, the main interest of the Security Service will not ordinarily be to prosecute the foreign intelligence officer who may have committed the offence. An attempt may be made to 'turn' the intelligence officer into a double agent or to have him declared *persona non grata* by the Department of External Affairs, or otherwise to neutralize his effectiveness while at the same time preserving the source's cover.

20. The practice of using undercover operatives in police and security intelligence work is well established in Canada and represents an important and valuable technique in criminal and security investigations. In the Supreme Court of Canada decision in *Kirzner* v. *The Queen*, Chief Justice Laskin referred to the use of spies and informers as "an inevitable requirement for the detection of consensual crimes and of discouraging their commission."[1] The Home Office in England expressed similar sentiments in a 1969 statement:

[1] [1978] 2 S.C.R. 487 at p. 493.

If society is to be protected from criminals, the police must be able to make use of informants in appropriate circumstances. Informants, appropriately employed, are essential to criminal investigations...[2]

21. The Report of the Canadian Committee on Corrections stated that:

> One of the most important aspects of police work in the field of crime prevention and the detection and apprehension of offenders involves the gathering of information with respect to intended crimes and the organization of criminal groups.
>
> ...Traditionally, information as to intended crimes has been obtained from informers and undercover agents.[3]

22. In a recent statement, Mr. Philip B. Heyman, Assistant Attorney General, Criminal Division of the United States Department of Justice, referred to undercover techniques as a "... minimally intrusive, powerfully effective weapon to detect, combat and deter the most serious forms of crime...".[4]

23. United States Attorney General Edward Levi, in 1976, noted in setting forth guidelines on F.B.I. use of informants in domestic security and criminal investigations that informants may often be essential to the effectiveness of properly authorized law enforcement investigations.[5] A number of other American studies have stressed the importance of the human source in criminal, particularly drug, investigations.[6]

24. In the R.C.M.P. Security Service, the use of undercover operatives is greatest in investigating domestic groups in Canada. A senior Security Service official stated to us, in the course of a briefing on the subject in February 1980, that undercover operatives are the "bread and butter" of Security Service operations. The vital importance of information provided to a security intelligence agency cannot be stated better than it was by the Royal Commission on Security:

> 285. All security activities depend upon information. The adequacy of appreciations and judgments can be no better than the information available. Without accurate and full information, the perception of the threat by the security authorities, and thus by the government whom they advise, will be less than satisfactory. Unimportant threats may be overemphasized, significant threats may be overlooked, and vital counter-measures may not be taken.

---

[2] The guidelines were contained in the *Home Office Consolidated Circular to the Police on Crime and Kindred Matters*, (Section 1, para. 92).

[3] Report of the Canadian Committee on Corrections, *Toward Unity: Criminal Justice and Corrections*, Ottawa, 1969, at p. 75.

[4] Testimony before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary — House of Representatives (March 4, 1980).

[5] *Attorney General's Guidelines for F.B.I. Use of Informants in Domestic Security, Organized Crime, and Other Criminal Investigations*, Washington, December 15, 1976.

[6] See e.g., J.H. Skolnick, *Justice Without Trial: Law Enforcement in Democratic Society*, New York, John Wiley & Sons, 1966, at p. 133; J. Wilson, *The Investigators: Managing F.B.I. and Narcotics Agents*, New York, Basic Books, 1978, at p. 58.

> 288. Human agents are one of the traditional sources of intelligence and security information, and any security service is to a large extent dependent upon its network of agents, on the scale of their penetration of or access to useful targets and on their reliability. Operations involving human sources require the most sophisticated handling by trained men with wide experience. Nevertheless, in spite of the difficulties associated with some of these operations, we regard them as essential to an effective security posture. We would go further, and suggest that it is impossible fully to comprehend or contain the current threats to security — especially in the field of espionage — without active operations devoted to the acquisition of human sources.[7]

We accept and endorse these statements emphasizing the utility of undercover operatives. Next we turn to violations of the law that have stemmed from these undercover operations during recent years. Before proceeding, however, we wish to note that since the Supreme Court of Canada's judgment in the *Kirzner* case there has been a view at very high levels of the R.C.M.P. that Chief Justice Laskin's language in that case is authority for the commission of offences by R.C.M.P. informers. In our opinion there is nothing in Chief Justice Laskin's judgment that supports the view that illegal conduct by an informer is or will be countenanced by the law.

B. LEGAL AND POLICY ISSUES ARISING FROM THE ACTIVITIES OF UNDERCOVER OPERATIVES

25. In this section, we shall examine possible violations of federal, provincial and municipal laws which may have been committed in the course of undercover operations and civil wrongs which may have occurred during such operations. These potential illegalities fall within the following general categories:

(a) violations of laws which require the accurate identification of persons and property;

(b) breaches of statutes such as the Income Tax Act, the Canada Pension Plan Act, and the Criminal Code arising out of payments made to sources and the encouragement of sources not to declare as income payments received from the Force for work on its behalf.

(c) violations of the Criminal Code and provincial laws during acts done to gain acceptance or maintain credibility with target groups;

(d) the breach of statutory prohibitions against possession and delivery of controlled or restricted substances or narcotics by undercover operatives investigating drug offences;

(e) violations of laws forbidding breach of trust by public officers and interference with confidential relationships as a result of practices connected with the recruitment and treatment of sources;

(f) offences under the Criminal Code which may occur through the removal of the property of others by an undercover operative and its delivery to the police;

(g) civil wrongs.

---

[7] *Report of the Royal Commission on Security*, Ottawa, 1969.

Each of these areas will be considered separately.

(a) *False documentation and registration*

26. In the previous chapter we examined the use of false identification documents (support documentation) in relation to physical surveillance operations, where such documents were needed to maintain an operation's secrecy. An even greater need for support documentation arises in the use of undercover operatives. Some targets of the Security Service and, increasingly, suspects in criminal investigations go to considerable lengths to verify the identity of individuals who seek to gain access to their organizations. Convincing support documentation is essential. To disguise effectively an operative's identity is not only a strategic necessity, it is essential for the physical safety of the operative, both during the actual operation and afterwards when it is sometimes necessary to relocate a threatened operative and to provide him with a completely new identity. We may comment further in a future Report on the need to protect the identity of sources, but at this time we withhold our comments pending the decision of the Supreme Court of Canada in *Solicitor General et al* v. *The Royal Commission of Inquiry with respect to the Confidentiality of Health Records in Ontario et al.*[8]

27. As explained earlier, the need for false documentation arises primarily in long-term, deep-cover operations. Casual sources do not ordinarily disguise their true identities; only their affiliation with the R.C.M.P. is kept secret. There is nonetheless an occasional need for false identification even for casual sources. When meeting, frequently in hotels, sources and their handlers have misrepresented their identities in order to avoid detection by their targets, who may have checked hotel registers and bribed hotel managers in order to obtain information about encounters with Criminal Investigation Branch or Security Service officers. Meetings between a member of the Security Service and a potential defector provide one example of the type of operations which have been kept secret, both for diplomatic and operational reasons.

28. The kind of support documentation used varies with the operation involved. Several common types of false documentation have been brought to our attention. They include:

— driver's licences
— S.I.N. cards
— passports
— credit cards
— motor vehicle registrations
— licence plates
— birth certificates
— education certificates

[8] The decision of the Ontario Court of Appeal, dated May 10, 1979, has not been reported.

29. The use of false documentation has resulted in the commission of a number of offences by undercover operatives, and by their handlers. These offences relate primarily to provincial highway traffic legislation (drivers' licences, licence plates, vehicle registrations), provincial hotel registration legislation (requiring registration in the guest's proper name) and a number of Criminal Code offences relating to forgery. In the previous chapter we examined in some detail these same legal difficulties as they arose in the context of physical surveillance operations. The issues here, for the most part, are identical, except that the broader range of identification documents necessary for undercover operatives means that more statutes may have been violated. In addition, one offence that we did not consider a problem in physical surveillance operations poses one in undercover operations because of the greater variety of cover or support documentation needed. It arises when documents for undercover operatives may have been obtained to substantiate the operative's cover story as to his date and place of birth, his supposed marriage etc.. If the documents were forged or if the documents were obtained through making a false statement in an application, and a record of such false information was inserted in a register, an offence may have been committed by those who caused the entry to be made. Section 335 of the Criminal Code reads:

> 335. (1) Every one who unlawfully
>
> (b) inserts or causes to be inserted in a register. . . an entry, that he knows is false, of any matter relating to a birth, baptism, marriage, death or burial, or erases any material part from such register...
>
> ...
>
> is guilty of an indictable offence and is liable to imprisonment for five years.

(b) *Complying with fiscal statutes relating to employer-employee relationships*

(i) Non-declaration of income and non-payment of tax

30. Sources may have been given a number of concessions in exchange for their assistance. The payment of money is a practice by police and security forces in many countries. The Security Service policy reflects the widespread acceptance of this practice:

> The secret expenditure of public funds on human source operations is recognized as a legitimate and necessary practice in the pursuit of intelligence gathering. It would not be possible to acquire a sufficient number of sources without provision to compensate them for their efforts and expenses.

Yet payments to sources threaten to reveal their covert role. Hence, care has been taken to ensure that payments do not attract attention. While the C.I.B. has no policy in this regard, Security Service policy until 1977 had been that sources should be instructed never to include payments in calculating taxable income. The policy read:

> All sources should be warned that any monies received from the Security Service must *never* be declared as income on their income tax returns. However, if part or all of such monies is retained in a manner which pays interest, such interest must be declared to avoid the attention of the tax department.

The policy was cancelled in November 1977, when its propriety came under review.

31. It is an offence under section 239(1) of the Income Tax Act for an individual to make false or deceptive statements in his income tax return. Where Security Service officers have advised their sources not to declare payments from the Force as income, those officers may have committed an offence.

(ii) *Employment relationship betwen R.C.M.P. and sources*

32. There are other statutes which require an employer to deduct money from remuneration due and to remit it to government. An example is the Canada Pension Plan Act. The R.C.M.P. has acted as if no source is ever an employee for the purposes of such statutes. While we have no doubt that that view is correct in law in regard to most sources, we also are convinced that in some cases a source is an employee of the R.C.M.P. within the meaning of the general law and the statutes in question. For example, Warren Hart was a paid full-time source of the R.C.M.P. Security Service from 1971 to 1975. We think that the tests that the law applies to determine whether a person is an employee (not an independent contractor) were satisfied in his case: the Security Service could order or require what was to be done, as to the details of the work; his work was an integral part of the "business" of the Security Service, not merely accessory to it; he was "part and parcel of the organization"; and he put his personal services at the disposal of the R.C.M.P. during some period of time and did not merely agree to accomplish a specified job or task.[9] We consider that the R.C.M.P. should address these issues in this light and recognize that non-payment and non-disclosure, particularly in the case of full-time sources, may give rise to breaches of the law. In Part V, Chapter 4 we shall make recommendations that the government should seek legislative amendments to overcome these practical difficulties — amendments similar to those referred to above in regard to the declaration of income tax.

(c) *Acts done to gain acceptance or to maintain credibility*

33. The most significant and intractable problem which arises in undercover operations, particularly those carried out by the Security Service, is the commission of unlawful acts by operatives in order to gain or maintain acceptance by the targetted individual or group. Sometimes, it is only by

---

[9] These tests are found in such cases as *Collins* v. *Herts County Council* [1947] K.B. 598; *Lambert* v. *Blanchette* (1926) 40 Q.B. 370 (Que. C.A.); *Stevenson London and Harrison Ltd.* v. *Macdonald and Evans* [1952] 1 T.L.R. 101 at 111 (Eng. C.A.); *Bank Voor Handel en Scheepwaart* v. *Stratford* [1953] 1 Q.B. 248 at 295 (Eng. C.A.); *Alexander* v. *M.N.R.* [1970] Ex. C.R. 138 at 153 (Exch. Ct.).

engaging in such conduct that the operative will advance to responsible positions within a target group, and therefore increase his access to valuable information.

34. A useful example is afforded by a case which came to public notice in 1977 when a long-term, deep-cover operative placed by the Security Service gave evidence at the trial of criminal charges laid against leaders of the Western Guard Party. The Western Guard Party professed an extreme ideology of which the chief tenets were racism, anti-Semitism and strident anti-Communism. It was suspected of being responsible for a rash of spray paintings which had defaced public and private property in Toronto in the early and mid-1970s. More seriously, the Security Service suspected in 1975 that the Western Guard planned to disrupt the 1976 Olympic Games, some of which were to be held in Toronto. That the Toronto segments included a soccer game involving the team from the State of Israel lent a particular urgency to the investigation. The Security Service recruited Robert Toope, who had come to its notice by reason of stories in the press concerning his anti-union activity at his place of business. With a view to using that publicity as a foundation for his cover story in applying to join the Western Guard, the Security Service sent Mr. Toope to Western Guard headquarters, where he was accepted and given membership. Mr. Toope testified at the trial of the accused that his involvement in the Western Guard Party fell roughly into four phases:

(i) The first phase included his initial penetration, his acceptance as a member and then as a group leader, his involvement in the distribution of the Guard's literature and then in pasting its posters on public sites, all of which occurred between May and September or October 1975.

(ii) Immediately thereafter, two events occurred which signalled the second phase of his penetration, deepened his involvement and led to his participation in acts and conspiracies of a more serious sort. The first event was the arrival of one "A", a new member who had a penchant for aggressive, violent behaviour. The second was the issuance of instructions by the Guard's leader to engage in a broader category of crime. Thereafter and through the late autumn of 1975 until February of 1976, Mr. Toope took part with "A" in spray painting incidents, and acted as a driver on occasions when "A" threw bricks through windows. As Mr. Toope became more and more concerned about "A's" propensity for violence and his increasingly uncontrollable behaviour, he expressed to his handler a desire to reduce his involvement. As a result, in about February of 1976, Mr. Toope told the Guard's leader that he no longer wished to accompany "A" on his missions. He gave as his excuse his concern for his family's welfare should he be caught.

(iii) In the weeks following, the quantity and quality of Mr. Toope's information waned. In about March 1976, the source and his handler decided that he should broaden his role again, but within certain limits. Specifically, it was agreed that Mr. Toope would attempt not to go out with "A", but rather would try to involve other members in such expeditions, with the hope that the presence of others would discourage "A's" impulsive and

dangerous tendencies. As well, Mr. Toope and his handler agreed that if he was to be involved at all in acts such as throwing objects through windows, his involvement would be strictly limited to driving the others to the scene.

(iv) In this fourth and last phase of Mr. Toope's involvement, he won once again the trust and confidence of the group. He was therefore able to obtain information which led to the arrest of the members before they had an opportunity to disrupt the Olympic soccer game at Varsity stadium. The Guard group had planned to throw smoke bombs onto the field during a game between the Israeli team and a team from South America.[10]

35. While unlawful acts to gain admission or enhance credibility pose problems in undercover operations on both the criminal investigation and Security Service sides of the Force, senior officers in the criminal investigation side have reported that such violations in their work have been limited primarily to drug investigations, and result from the narrowness of the statutory exemptions available in the Narcotic Control Act and the Food and Drugs Act for police and persons acting pursuant to their instructions. (For a discussion of those violations, see below.)

36. In order to determine the extent and prevalence of such unlawful acts on the Security Service side, the Commission asked the present Deputy Director General (Operations) of the Security Service to request certain Area Commanders in the Security Service to assess the frequency with which such violations have occurred in the past, and to give their opinion whether undercover operatives need to violate laws in order to work effectively. At our request a message to this effect was sent on February 22, 1980 to certain Area Commanders. We selected those Area Commands because they have been the areas in which most use has been made of undercover operatives in the past two decades, and they would therefore be the Area Commands most likely to be able to give us evidence as to "extent and prevalence". It asked how often in the past 20 years there had been a "real need" for undercover operatives to commit criminal acts, and whether there had been intelligence operations which could not be commenced because criminal acts were known to be required of new members in the target group. Area Commanders were also asked to survey members in their command and ex-members in order to identify cases which would illustrate the extent and prevalence of violations.

37. One Command identified eight operations in which undercover operatives had either committed violations or had been asked by the target group to do so. The violations included mischief to property, fraud, failure to declare income, and theft under $200.00. In one case, the source had been asked to obtain certain articles the possession of which is illegal. The source was instructed by his handlers to obtain some of the items and abided by that instruction. The source was not instructed regarding others because his handlers were confident that he would not become involved in the matter. In another case a source was

[10] Trial transcript, *Regina* v. *Andrews et al*, Criminal Assizes Court, Judicial District of York (Toronto, Ontario), 1977, before His Honour Judge Graburn and a jury.

asked by a target group to participate in a financial fraud. Group leaders eventually decided to involve a different individual, and it appears that in any event the fraud did not take place.

38. Another Area Command identified two cases in response to the inquiry from Headquarters. In one, an undercover operative committed theft under $200.00 in order to enhance his acceptance by a target group and was later credited with preventing the commission of a serious crime. In the second case, an undercover operative was directed by the target group to plan and carry out a physical assault upon an enemy of the group. When the advice of Headquarters was sought by the field office involved, indirect steps were counselled which would discourage the group leaders from pressing the attack, but it was acknowledged by one senior officer that it might well be necessary for the operative to carry out a simple assault in order to maintain his cover. The Area Command has advised us that "there is no indication on the source file that this was ever pursued further".

39. Another Area Command reported no new cases, saying that all such operations were already before this or other Commissions.

40. We have encountered additional cases in which undercover operatives have violated laws. In some, operatives took part in illegal demonstrations. In others, they purchased or possessed restricted weapons; purchased and possessed explosives without appropriate permits; obtained access to confidential information in contravention of the governing statute; committed mischief in relation to private and public property and caused wilful damage to property.

41. We wish to remark in particular about a practice which is common to both the Criminal Investigation Branch and the Security Service — participation by the undercover operative in the planning of a crime. From our reading of its policies, we have observed that the R.C.M.P. has been concerned that such conduct itself amounted to a violation of law (as the offence of conspiracy). We consider that such conduct is not unlawful so long as the operative does not intend to take part in the act being planned. The Supreme Court of Canada in *Regina* v. *O'Brien*[11] held that a mere agreement to commit an indictable offence, without the intention to carry into effect the common design, is not sufficient to constitute the offence of conspiracy. For the operative to commit the offence of conspiracy, therefore, he would not only have to agree but also to intend to put the common design into effect. If the rest of the conspirators did so intend, they could be convicted of conspiracy.

(d) *The Food and Drugs Act*[12] *and the Narcotic Control Act*[13]

42. In drug investigations, an undercover member or source necessarily adopts the guise and mannerisms of individuals who typify the drug community. In the course of playing the part of an addict or trafficker, the undercover operative may be asked to handle, administer or deliver drugs. Criminal

[11] [1954] S.C.R. 666.
[12] R.S.C. 1970, ch.F-27.
[13] R.S.C. 1970, ch.N-1.

investigation officers have repeatedly stressed that such acts are essential to attaining and maintaining credibility in the drug community. However, under existing law, such acts may, depending on the circumstances, result in the commission of drug offences by the operative.

43. Drug offences are defined in the Narcotic Control Act and the Food and Drugs Act. Section 3 of the Narcotic Control Act prohibits the possession of a narcotic. Section 4(1) of the Act provides that "no person shall traffic in a narcotic or any substance represented or held out by him to be a narcotic". Section 4(2) provides that "no person shall have in his possession any narcotic for the purpose of trafficking". The expression "traffic" means "to manufacture, sell, give, administer, transport, send, deliver or distribute", or to offer to do any of these activities. Section 5 of the Act states that except as authorized by this Act or the regulations, "no person shall import into Canada or export from Canada any narcotic". Section 34(1) of the Food and Drugs Act prohibits trafficking in a controlled drug or any substance represented or held out to be a controlled drug. Possession of any controlled drug for the purpose of trafficking is prohibited under section 34(2). In this section, the expression "traffic" means "to manufacture, sell, export from or import into Canada, transport, or deliver", otherwise than under the authority of Part III of the Act or the regulations. There is no offence of possession of a controlled drug *simpliciter*. Under section 41(1), it is an offence to possess a restricted drug. Section 42(1) prohibits trafficking in a restricted drug or any substance represented or held out to be a restricted drug, and section 42(2) prohibits possession of a restricted drug for the purpose of trafficking. The expression "traffic" has the same meaning as it does in the context of controlled drugs.

44. We now examine a number of problem situations which arise in connection with drug investigations as such problems were presented to us in meetings with senior officers from the R.C.M.P.'s Criminal Investigation Branch.

(i) The Commission or Kickback/Trafficking Situation: In making a purchase of narcotics directly from, or as a result of an introduction by a middleman, the undercover operative frequently has been expected to comply with the custom of the trade by giving a small percentage of the purchase to the middleman as a commission. Under present legislation, the undercover operative would be committing the offence of trafficking.

(ii) The Administering/Trafficking Situation: In the course of their associations with addicts, undercover members or sources (the latter of whom may themselves be addicts) have been asked by the addict to administer or assist in administering the drug. As in the "kickback" situation described above, administering a drug may constitute the offence of trafficking.

(iii) The Passing On/Trafficking Situation: Again, because of their required association with drug users, undercover operatives have been called upon to "take a joint" of marijuana, sniff cocaine, or even inject heroin. Undercover members have been instructed to simulate the act where possible or, if necessary, refuse the drug and pass it on. By passing on the drug, the undercover member may commit the offence of trafficking. Undercover sources, who may be regular users in any event, have been

given no instructions to simulate the use of the drug. Nonetheless, in passing on the drug, they may also have committed the offence of trafficking.

(iv) The Offering/Trafficking Situation: As part of establishing and maintaining credibility, undercover members have been *encouraged* to offer drugs for sale, but never to carry through such an offer by actually making a sale. This has been a regular operational practice. Undercover sources (who are sometimes established traffickers) have generally been allowed to operate as they normally would. Often this has meant that sources are permitted to continue their possession or trafficking of drugs. In the case of both members and sources, the offence of trafficking may have been committed.

(v) The Distribution/Trafficking Situation: The "controlled delivery" of narcotics is another operational technique which has raised questions of legality. In order to gain sufficient evidence or intelligence to implicate the principals in illicit drug organizations, decisions have been made to "sacrifice" an amount of drugs (normally only a small amount) for distribution to users in order to avoid the target's suspicion that would arise when a quantity of drugs destined for the "market" did not arrive. Evidence led at a recent British Columbia Supreme Court drug trial illustrates this operational technique.[14] C.I.B. handlers, after taking samples of a drug supplied to their source by the target, permitted the source to sell the remainder of the drug for this very reason. 'Sacrifices' have also occurred in 'Test Run' situations, where an international drug enterprise, having set up a major deal with an undercover operative to import drugs into Canada, will first run a comparatively small amount through the planned route before delivery of the main shipment. Where undercover operatives have become directly involved as couriers, they may have committed the offences of importing and trafficking.

(vi) Possession: Section 3(1) of the Narcotic Control Regulations[15] states in part:

> 3. (1) A person is authorized to have a narcotic in his possession where that person has obtained the narcotic pursuant to these Regulations and...
>
> (g) is employed as an inspector, a member of the Royal Canadian Mounted Police, a police constable, peace officer or member of the technical or scientific staff of any department of the Government of Canada or of a province or university and such possession is for the purposes of and in connection with such employment.

The apparent breadth of section 3(1) is limited by the requirement that the narcotic be obtained "pursuant to these Regulations". We do not think that when an undercover member comes into possession of a narcotic while investigating narcotic trafficking, he is protected by this section. While the member does have possession "for the purposes of and in connection with such

[14] Reported on appeal in *Regina* v. *Ridge*, (1979) 51 C.C.C. (2d) 261 (B.C.C.A.).
[15] C.R.C., ch.1041.

employment", he has not obtained the narcotic "pursuant to these Regulations". The Regulations provide protection only in the specific case of an R.C.M.P. member being supplied the narcotic by a licensed dealer (section 24(2)). A provision similar to section 3(1)(g) is included in the part of the Food and Drugs Regulations[16] dealing with restricted drugs. (It will be recalled that there need be no corresponding exemption in the case of a *controlled* drug, as possession of that drug is not an offence):

> J.01.002. The following persons may have a restricted drug in their possession:
>
> (c) an analyst, inspector, member of the Royal Canadian Mounted Police, constable, peace officer, member of the staff of the Department of National Health and Welfare or officer of a court, if such person has possession for the purpose and in connection with his employment.

Unlike the Narcotic Control Regulations, however, the Food and Drugs Regulation does not cover possession by sources. In addition to the exemptions described above for the possession of a narcotic, the Minister may, pursuant to the regulations, authorize possession of a narcotic as follows:

> 68. (1) Where he deems it to be in the public interest, or in the interests of science, the Minister may in writing authorize
>
> (a) any person to possess a narcotic,
>
> for the purposes and subject to the conditions in writing set out or referred to in the authorization.

These authorizations for possession of narcotics and restricted drugs must, however, be read in light of the comments of Mr. Justice Laskin, when he was still a member of the Ontario Court of Appeal, in *Regina* v. *Ormerod*.[17] At that time, the Regulation read as follows:

> An inspector, a member of the Royal Canadian Mounted Police, constable or peace officer or member of the technical or scientific staff of any department of the Government of Canada, of a Province or university, may be in possession of a narcotic for the purpose of, and in connection with, his employment therewith.

His Lordship limited the effect of the section (now section 3(1)(g) of the Narcotics Control Regulations, and similar to section J.01.002 of the Food and Drugs Regulations) by holding that the Regulation did not protect an undercover member of the R.C.M.P. who had purchased narcotics and therefore had "possession as a direct consequence of trafficking which ensues from solicitation by a policeman".[18] It may be argued nonetheless that the member and even his source would have a defence if charged with possession since the courts have held the offence of possession to involve a degree of *control* which would not be present if the possession was solely for the purpose of furthering the investigation and the person in possession had the immediate intention of turning the drug over to the police. In long-term undercover operations,

---

[16] C.R.C., ch.870.

[17] [1969] 4 C.C.C. 3, at p. 13.

[18] *Ibid.*, at p. 240.

however, it is not always the member's or source's immediate intention to turn the drug over to the police. The six operations described earlier in this paragraph, although they may be unlawful, have been referred to us by the R.C.M.P. as vital to the successful prosecution of drug-related offences.

(e) *Breach of trust and interference with confidential relationships*

(i) Section 111, Criminal Code of Canada

45. When a source who is the employee of a government discloses information which he is bound by his office to keep in confidence, the issue arises as to whether the source has thereby committed a breach of trust as that offence is defined by section 111 of the Criminal Code.

46. The concept of "breach of trust" in this context is very elastic and flexible. It includes any malfeasance in office. The leading case on the subject in Canada is *Regina* v. *Campbell*,[19] a decision of the Ontario Court of Appeal. That Court emphasized that there may be guilt even for negligence. From this it follows that it is not essential, in order to obtain a conviction, that the official have the intent to injure the government. In our view all that the prosecution need prove is that the official intended to do the act complained of — i.e. the communication of the information. It follows that it would be no defence that the official believed that he was acting in the public interest, or in the interest of national security. In *Regina* v. *Arnoldi*,[20] Chancellor Boyd said:

> The gravity of the matter is not so much in its merely profitable aspect as in the misuse of power entrusted to the defendant for the public benefit, for the furtherance of personal ends. Public example requires the infliction of punishment when public confidence has thus been abused. ...

Thus, payment for the information would enhance the probability that a prosecution would result in conviction. A source in government, paid monthly by a security intelligence agency for the provision of confidential information received by him because of his public position, would likely be guilty under this section unless the information were evidence of the commission of a crime. (In the latter case he would be carrying out a citizen's duty that is recognized by the law.) However, payment would not be necessary for conviction. It simply makes conviction more likely because the payment of money would lessen the possibility that a jury would be impressed by the protestation of the defence that what the official did was for love of country.

47. The foregoing conclusion applies whether the government in question is federal, provincial or municipal, provided that the information is of a type which it is his duty not to divulge. If the government in question were a provincial government, and the security intelligence organization asked an official of that government to report to it information concerning that government's dealings with foreign powers, no doubt it might be contended on behalf of the security intelligence organization, and on behalf of the official if he were prosecuted, that he was providing information concerning matters which, in the

[19] [1967] 3 C.C.C. 250.

[20] (1893), 23 O.R. 201 at p. 212.

circumstances, were not legitimate operations of a provincial government and were within the sole legitimate concern of the federal government. However, while a jury might not convict if it were satisfied that the official's concern was genuinely limited to protecting Canada against unacceptable foreign intervention, we still think it probable that an offence is committed in those circumstances.

48. Moreover, the information provided may inevitably stray from the narrow limits intended and include other confidential information about perfectly proper provincial government plans and policies. Plans and policies might be disclosed which concern matters under negotiation or future negotiation with the federal government, or the negotiations of provincial governments with foreign governments or private interests concerning economic matters. In that event, the argument that there is no offence committed evaporates, and in addition there is a very serious constitutional and political issue of a policy nature involved if the federal government through its security intelligence agency obtains confidential information about the policies and plans of a provincial government.

49. If an offence is committed by such a source, the members of the security intelligence organization handling the source, encouraging the source to provide such information and perhaps even paying him a regular honorarium, would be guilty either of conspiracy or of being accessories to the offence itself.

50. A second problem presented by section 111 arises when the R.C.M.P. refrains from bringing criminal charges so as not to compromise undercover operations.

51. Undercover operations often allow the R.C.M.P. to learn about crimes which the target has committed or plans to commit, but it is not always consistent with the objectives of the investigation immediately to arrest and charge the target with the known or anticipated offence or conspiracy. For example, an undercover operative in a drug investigation may observe scores of violations of drug laws among those he has infiltrated, but his handler may decide to await a larger, more serious transaction before arranging the arrest of those responsible. Even then, some offenders may never be charged, because the Force intends to use them as unwitting tools in order to acquire evidence against "more important" offenders. This practice is known as "targetting upwards". On the security side, an operative may report on crimes committed by a target over a period of years without charges being laid, since the object of his mission may be to obtain continuous intelligence information about a long-term threat to security.

52. All R.C.M.P. members are sworn to an oath of office which requires them both to obey their lawful orders and "faithfully, diligently and impartially" to perform their duties. Since their duties include those assigned to peace officers in the preservation of peace, the prevention of crime and offences against the law and the apprehension of criminals and offenders, the question arises whether they violate section 111 by enforcing laws "selectively". Section 111 of the Criminal Code of Canada reads as follows:

> Every official who, in connection with the duties of his office, commits fraud or a breach of trust is guilty of an indictable offence and is liable to imprisonment for five years, whether or not the fraud or breach of trust would be an offence if it were committed in relation to a private person.

The Supreme Court of Canada has held that section 111 of the Code applies to a person who holds an office within the definition of that word in section 107[21] and also a person holding an office within the usual meaning of the word "office". The Court took notice of the broader dictionary definition which is, in part, "A position of duty, trust or authority, especially in the public service, or in some corporation, society or the like" (per Chief Justice Fauteux, in *Regina* v. *Sheets*[22]). It is therefore beyond doubt that a member of the R.C.M.P. is an "official" within the meaning of that word as used in section 111 of the Code. Given that fact, is omitting to enforce the criminal law immediately upon learning of each and every crime a "breach of trust... in connection with the duties of his office..."?

53. The phrase "breach of trust" as it appears in the section has been given a broad, non-technical interpretation by the Courts. Its meaning is not confined to the rules and concepts of the law of trusts and fiduciaries. Nor is there any requirement that there be a "trust property". In the case of *Regina* v. *Campbell*,[23] the Court of Appeal for Ontario said:

> In our opinion s.103 [now 111] is wide enough to cover any breach of the appropriate standard of responsibility and conduct demanded of the accused by the nature of his office as a senior civil servant of the Crown... The question which will have to be determined and which has not been considered is whether Campbell by reason of his dealings and actions abused the public trust and confidence which had been placed in him by his appointment as a servant of the Crown and thereby did he or did he not commit a breach of trust in relation to his office?

A later passage in the same judgment makes it clear that the Court of Appeal accepted the term "trust" in its widest sense:[24]

> The situation has been very tersely summed up in the United States. For example, in the American Words and Phrases, Permanent Edition, Vol. 29, p. 250, there is the following note:
>
> "An 'office' has been defined as 'a special trust or charge created by competent authority'; more tersely still 'a public office is a public trust.' ... *Gracey* v. *City of St. Louis*, 111 S.W. 1159, 1163."

---

[21] Section 107 defines "office" as follows:

> "office" includes
>
> (a) an office or appointment under the government,
>
> (b) a civil or military commission, and
>
> (c) a position or employment in a public department,

[22] (1971) 1 C.C.C. (2d) 508 at 513.

[23] [1967] 3 C.C.C. 250.

[24] *Ibid.*, at p. 257.

> The respondent suggests that the possible use of the word "trust" to implicate "confidence" is a colloquial usage. While it is perfectly true that the term "trust" is a term of art in the legal field of equity the Shorter Oxford Dictionary at p. 1362, gives the following meaning for the word "office":
>
> 4. A position to which certain duties are attached, especially a place of trust, authority or service under constituted authority, M.E. e.g. The Office of Coroner.

54. There are many ways in which a public official can breach his trust in office. He may accept a bribe, or neglect his job through laziness. Those types of breach of trust are not relevant to the present discussion. Rather, the question for present consideration is whether a deliberate omission to enforce the law in certain circumstances may constitute a breach, notwithstanding that it is motivated by the honest belief by the officer that he is acting in the best interests of the public.

55. The English Court of Appeal has had occasion in recent times to consider this question in *R.* v. *Metropolitan Police Commissioner, ex parte Blackburn*, (Blackburn No. 1)[25] and *R.* v. *Metropolitan Police Commissioner, ex parte Blackburn*, (Blackburn No. 3).[26] In *Blackburn No. 1* Mr. Blackburn sought mandamus against the Metropolitan Police Commissioner to compel him to enforce certain gaming and betting laws. A confidential instruction had been issued by the Commissioner to senior officers of the London Metropolitan Police, containing a policy decision not to prosecute gambling clubs for breach of the gaming laws unless there were complaints of cheating or the clubs had become the haunts of criminals. In the court of first instance, Mr. Blackburn sought mandamus for three heads of relief. On appeal, he pursued only the third head — a reversal of the policy decision embodied in the special instruction. The Court of Appeal held that it was the duty of the Commissioner and also of chief constables to enforce the law; though chief officers of police have discretion — for example, whether to prosecute in a particular case — the court might interfere in respect of a policy decision amounting to a failure of the duty to enforce the law. The following statements of Lord Denning, M.R. are of interest:[27]

> I hold it to be the duty of the Commissioner of Police, as it is of every chief constable, to enforce the law of the land. He must take steps so as to post his men that crimes may be detected; and that honest citizens may go about their affairs in peace. He must decide whether or not suspected persons are to be prosecuted; and, if need be, bring the prosecution or see that it is brought; but in all of these things he is not the servant of anyone, save of the law itself. No Minister of the Crown can tell him that he must, or must not, keep observation on this place or that; or that he must, or must not, prosecute this man or that one. Nor can any police authority tell him so. The responsibility for law enforcement lies on him. He is answerable to the law and to the law alone.

---

[25] [1968] 1 All E.R. 763 (C.A.).

[26] [1973] 1 All E.R. 324 (C.A.).

[27] *Ibid.*, at p. 769.

> Although the chief officers of police are answerable to the law, there are many fields in which they have a discretion with which the law will not interfere. *For instance, it is for the Commissioner of Police, or the chief constable, as the case may be, to decide in any particular case whether enquiries should be pursued, or whether an arrest should be made, or a prosecution brought.* It must be for him to decide on the disposition of his force and the concentration of his resources on any particular crime or area. No court can or should give him direction on such a matter. He can also make policy decisions and give effect to them, as, for instance, was often done when prosecutions were not brought for attempted suicide; but there are some policy decisions with which, I think, the courts in a case can, if necessary, interfere. Suppose a chief constable were to issue a directive to his men that no person should be prosecuted for stealing any goods more than £100 in value. I should have thought that the court could countermand it. He would be failing in his duty to enforce the law. (Our emphasis.)

56. A similar issue arose in respect of police discretion in *Blackburn No. 3*. There Mr. Blackburn moved for an order of mandamus to direct the Commissioner to secure the enforcement of the law relating to obscene materials and to reverse the decision of the Commissioner that no police officers would be permitted to prosecute offenders against those laws without the prior consent of the Director of Public Prosecutions. The Court of Appeal held that, although the evidence disclosed that obscene material was widely available, the applicant had not established that it was a case for the court to interfere with the discretion of the police in carrying out their duties. Lord Denning, M.R. concluded that:[27]

> . . . the police have a discretion with which the courts will not interfere. There might, however, be extreme cases in which he was not carrying out his duty. And then we would. I do not think this is a case for our interference. In the past the commissioner has done what he could under the existing system and with the available manpower. The new commissioner is doing more. He is increasing the number of the Obscene Publications Squad to 18 and he is reforming it and its administration. No more can reasonably be expected.

57. From the foregoing principles and authorities, we draw the following two conclusions. First, generally, the decision in a given case to forbear in charging an offender where investigation is continuing in respect of other offences adjudged by the police as more serious, or in respect of other activities assessed to be a greater threat to Canada, is a proper exercise of a peace officer's discretion and will not constitute a breach of trust in connection with the duties of his office, provided that the discretion is exercised in good faith and for proper motives. Second, it will be otherwise where the forebearance amounts to a complete failure to enforce the law, as, for example, where a known trafficker in drugs is allowed indefinitely to continue in his crime with impunity, to the knowledge of the police. We are enquiring into certain instances in which it has been alleged to us that the R.C.M.P. has allowed a source who is a known trafficker in drugs to continue trafficking with impunity upon the condition

[28] *Ibid.*, at pp. 331-2.

that he provide information about others when asked. In a future report we shall consider those allegations in detail and make recommendations as to what the practice should properly be.

(ii) Section 383, Criminal Code of Canada

58. By virtue of section 383(1) of the Criminal Code of Canada, it is an offence "corruptly" to give any form of benefit to an agent or employee in exchange for that person doing any act or showing any favour in relation to the principal's or employer's affairs or business. The issue arises whether in those cases in which the R.C.M.P. has obtained information from a paid undercover operative who is also an employee or agent, and in which the information related to the principal's or the employer's business, the R.C.M.P. has committed the offence created by section 383(1).

59. Section 383 of the Code is entitled "Secret Commissions — Privity to Offence — Punishment — Definitions". It appears in Part VIII of the Code, which is entitled generally "Fraudulent Transactions Relating to Contracts and Trade". The section itself reads as follows:

> 383. (1) Every one commits an offence who
>
> (a) corruptly
>
> (i) gives, offers or agrees to give or offer to an agent, or
>
> (ii) being an agent, demands, accepts or offers or agrees to accept from any person,
>
> a reward, advantage or benefit of any kind as consideration for doing or forbearing to do, or for having done or forborne to do, any act relating to the affairs or business of his principal or for showing or forbearing to show favour or disfavour to any person with relation to the affairs or business of his principal...
>
> (2) Every one commits an offence who is knowingly privy to the commission of an offence under subsection (1).
>
> (3) A person who commits an offence under this section is guilty of an indictable offence and is liable to imprisonment for two years.
>
> (4) In this section "agent" includes an employee, and "principal" includes an employer.

The offences generally resemble those dealing with bribery of public officials created by sections 110 and 112 of the Code, and appear to be intended to discourage similar evils respecting private master-servant and principal-agent relationships.

60. In order for the offence to be committed, it need not be shown that the giving of the information or the act done by the agent was in any sense injurious to the principal's affairs, or even contrary to his best interests. It would appear that the interest sought to be protected is the integrity of the relationship itself, and that the gist of the offence is that a third party subverts that integrity by paying the agent to do an act affecting the relationship.

61. It is also noteworthy that the offence lies not in the performance of the act or the exercise of favour but rather in the corrupt offer of or demand for

reward. The act of the agent might itself be entirely proper, and indeed form part of the lawful duties which he is bound to perform. Nevertheless, an offence is committed if reward is given in consideration of the act or forbearance.

62. In part, the section codifies the common law with respect to the fiduciary obligations of agent and servant — specifically that they should receive no secret profit or benefit. The receipt of a reward or benefit, and perhaps the mere demand by the fiduciary for such an advantage, is a tortious breach of his duty. However, it cannot be any breach of duty on the part of the agent or employee if a third person offers him a secret advantage which he refuses, although the third person may be criminally liable pursuant to section 383(1) of the Code.

63. Sections of the Code which prohibit bribery of those in public positions refer only to the giving and accepting of benefits and rewards: the adverb "corruptly" does not appear, as it does in section 383(1). It would at first appear that the word "corruptly" contained in section 383(1) adds an element to the offence which would be lacking in the conduct of a police or security officer in bribing an agent to inform on his principal. The defence would rest upon the higher motive and lofty intent which inspired the bribe, the conduct amounting to anything but "corruption". That defence is not available, however, since there is clear and strong authority in Canada that the word "corruptly" does not add an element which must be proven to establish guilt; rather, the word is redundant, since the act which is prohibited by the section has been held to be intrinsically corrupt and so cannot be done under innocent or extenuating circumstances. Perhaps the clearest illustration of the judicial interpretation placed upon the section is afforded by *R.* v. *Brown*.[28] In that case, Mr. Justice Laidlaw, of the Ontario Court of Appeal, turned his attention to the purpose for which the section was enacted:

> The evil against which that provision in the Criminal Code is directed is secret transactions or dealings with a person in the position of agent concerning the affairs or business of the agent's principal. It is intended that no one shall make secret use of the agent's position and services by means of giving him any kind of consideration for them. The agent is prohibited from accepting or offering or agreeing to accept any consideration from anyone other than his principal for any service rendered with relation to the affairs or business of his principal. It is intended to protect the principal in the conduct of his affairs and business against persons who might make secret use, or attempt to make such use, of the services of the agent. He is to be free at all times and under all circumstances from such mischievous influence. Likewise, it is intended that the agent shall be protected against any person who is willing to make use secretly of his position and services... In my opinion, the act of doing the very thing which the statute forbids is a corrupt act within the meaning of the word "corruptly" used in the section under consideration. I think that word was

[29] The cases which have considered the section are *R.* v. *Gross*, [1946] O.R. 1; *R.* v. *Brown*, [1956] O.R. 944 and *R.* v. *Reid*, [1969] 1 O.R. 158, all of which are decisions of the Court of Appeal for Ontario.

> intended to designate the character of the act prohibited by the legislation. If a person were to give a sum of money, secretly, to an agent for the very purpose of having him do some act... it could not be said that he did not intend to contravene the provisions of section 368[383], or that he acted honestly or in good faith. It must be held that he intended to do the very thing Parliament intended to prohibit. His act can be regarded only as a corrupt act. In my opinion, it is not an answer in law for a person to say that he believed he had a right to have a certain thing done by an agent's principal, or that he believed that the agent ought to have done the act in question with relation to the affairs or business of his principal. His belief in respect of his rights does not justify his doing the very act intended to be prohibited by law.[30]

Mr. Justice Gibson, dissenting, would have concurred in the result on the evidence but differed on the meaning of the word "corruptly". He was unable to agree that a payment honestly made would be corrupt, merely because it amounted to the very act otherwise described in section 383. He referred to the common dictionary definition of "corrupt", and concluded that at the least, an act done "corruptly" is done with an evil mind — with evil intention, and except where there is an evil mind or intention accompanying the act, it is not done corruptly. He concluded:

> From the definitions it is difficult to understand how a corrupt act could be honestly performed.
>
> If the interpretation placed upon s.368[383] by the trial judge when he recalled the jury is correct the word "corruptly" in the section is superfluous, and any payment to an agent for doing or forbearing to do any act relating to the affairs or business of his principal is automatically an offence — whether such payment is made with honest intentions or dishonestly.
>
> This, in my opinion, goes beyond the true intent of the statute.[31]

64. The rationale underlying Mr. Justice Gibson's dissenting view in *Brown* was rejected by the English Court of Appeal in *R.* v. *Smith*.[32] There, the accused had offered a bribe to a public official. When charged, he raised the defence that he had done so with the altruistic intention of subsequently exposing the corrupt public servant. It was held that his ulterior motive was irrelevant. The accused acted "corruptly", as that word appeared in the statute, because he deliberately did an act — i.e. conferred a benefit upon a person in a defined class — which the statute forbade. In delivering the judgment of the Court, Lord Parker, Lord Chief Justice, concluded that the object of such legislation was to prevent public servants from being subjected to temptation. The very act of offering was prohibited, and the word "corruptly" added nothing to the Crown's burden in making out a case.

65. A second line of authority, emanating from English and Australian courts, attaches some significance to the word "corruptly". In an Australian case, *Rex* v. *Stevenson*,[33] Mr. Justice Hood considered the meaning of the word

[30] [1956] O.R. 944 at p. 946.
[31] *Ibid.*, at p. 962.
[32] [1960] 1 All E.R. 256.
[33] [1907] V.L.R. 475 at 476. (S.C. of Victoria).

"corruptly" in the Secret Commissions Prohibition Act, 1905 and concluded that in that Act, "corruptly" must mean some wrongful intention. In *C.* v. *Johnson*,[34] the Supreme Court of South Australia examined the meaning of the word "corruptly" in the Secret Commissions Prohibition Act, 1920. Mr. Justice Travers stated:

> On normal legal principles one would expect that word [corruptly] to add something to the meaning of the section... I think that this statute does import that the defendant was acting *mala fide*... and with wrongful intention...
>
> My view is that the commission of an offence against [the Act] necessarily involves dishonesty, and that a man who acts corruptly within the meaning of that section [of the Act] necessarily acts dishonestly.[35]

66. English decisions have also illustrated an inclination to attribute some meaning to the word "corruptly". Although Mr. Justice Willes in the 1858 decision in *Cooper* v. *Slade*[36] indicated that the word "corruptly" in an election statute did not mean "dishonestly", a number of subsequent cases have imported some notion of dishonesty when the word "corruptly" appeared. In *Bradford Election Petition — No. 2*,[37] Baron Martin stated that the word "corruptly" meant "an act done by a man knowing that what he does is wrong, and doing so with evil feelings and with intentions". More recently, in *R.* v. *Lindley*,[38] D Mr. Justice Pearce interpreted the word "corruptly" in the Prevention of Corruption Act, 1906 to require a dishonest intention. In *R.* v. *Calland*,[39] Mr. Justice Veale referred to *Lindley* and directed a jury considering that same Act that "corruptly" meant dishonestly. The *Calland* case, decided in 1967, may not, however, have taken into account the 1960 decision of the English Court of Appeal in *R.* v. *Smith*.[40]

67. It can be seen that the Australian courts have imported an element of dishonesty into the word "corruptly". English courts have wavered, but it is submitted that the Court of Appeal decision in *Smith* resolves the issue; the word "corruptly" imports no notion of dishonesty. The subsequent decision in the *Calland* case may be regarded as having been made *per incuriam*. In any event, the questions raised by the interpretation of "corruptly" have clearly been resolved in Canada. In Canada, the word "corruptly", at least as used in section 383, is redundant. We submit that this is the proper interpretation, since the very act of rewarding an agent or employee for doing something in connection with his principal's or employer's business violates the integrity of a relationship that is sought to be protected.

68. We pass to the question whether any defences are available to R.C.M.P. members who have paid agents to do an act or show favour with relation to

---

[34] [1967] S.A.S.R. 279 (S.C.).
[35] *Ibid.*, at p. 291.
[36] 6 H.L.C. 746 at 773.
[37] (1869), 19 L.T.R. 723 at 727.
[38] [1957] Crim. L.R. 321 (Lincolnshire Assizes).
[39] [1967] Crim. L.R. 236 (Lincolnshire Assizes).
[40] [1960] 2 Q.B. 423.

their principal's affairs. Where the principal or employer is engaged in crime, there is no lawful relationship the integrity of which is worthy of protection; no crime is committed should the agent or employee pass information for pay to the R.C.M.P. Although there are no cases which have considered this point, we do not interpret section 383(1) as protecting relationships tainted by a criminal object. Similarly, we consider that section 383(1) has no application where the information conveyed by the agent or employee, even when it affects the lawful affairs of his principal, provides evidence of a crime. The difficult issue in this context is whether section 383(1) is violated when the R.C.M.P. pays an agent or employee to report about the lawful business or affairs of his principal or employer, and no evidence of a crime is produced thereby. There have been circumstances in which the R.C.M.P. (and particularly the Security Service) have solicited and received such information in relation to its role in gathering intelligence. Is an offence thereby committed? If so, are there defences available?

69. We first consider motive. It may be argued that the act was performed with a higher purpose in mind. Courts in Canada, Britain and the United States have repeatedly held that "the criminal nature of an act is not purged by good motive...".[41] Glanville Williams cites the Criminal Law Commissioner's 7th Report (1843):

> To allow any man to substitute for law his own notions of right, would be in effect to subvert the law.

Even in the United States, where certain punitive provisions have been held not to apply to police officers executing their duties, altruistic intention or motive is no defence to crime.[42] A crime is a crime although committed for the ultimate purpose of enforcing the law.[43] This issue is dealt with more fully in Part IV.

70. Similarly, we consider that defences are not afforded upon the principles of Crown immunity or public policy; nor do we feel section 25 of the Criminal Code provides an answer to such a charge. The common law defence of necessity is also not available in such circumstances, as the practice of paying secret commissions is merely one of a variety available to the Force to gather information about a given subject. It cannot be said to be a "necessary" technique, although it is undoubtedly an effective one. These issues are also discussed in detail in Part IV.

71. Thus, there may have been violations of section 383 of the Criminal Code where the R.C.M.P. has given, or has offered or agreed to give a reward, advantage or benefit to an agent or employee of a principal or employer, in consideration of that person furnishing information concerning the business or affairs of his principal or employer, unless that information was evidence of the commission of a crime.

---

[41] Glanville Williams, *Criminal Law: The General Part*, 2nd ed., London, Stevens, 1961, at 748.

[42] *People* v. *Williams*, (1952) 113 N.Y.S. (2d) 167.

[43] *Hamp* v. *State of Wyoming*, 118 P. 653. See generally *Corpus Juris Secundum*, Criminal Law, Vol. I, pp. 9ff.

72. If the law does make the furnishing of such information an offence, the consequences from the point of view of the gathering of criminal intelligence (which may not provide evidence of a crime or of an unlawful business activity) by any police force — not just the R.C.M.P. — are seriously adverse to effectiveness, if the police force is expected to remain within the law. Similarly, the consequences from the point of view of the effectiveness of Canada's security intelligence agency are serious, if the agency is to be expected to use only lawful techniques. It would render impossible making payments to certain sources engaged in a counter-espionage investigation or paying a source who has penetrated a subversive organization and is in its employ in exchange for information about the affairs of the organization.

73. In the absence of further interpretation of section 383, it is not possible to define the limits of permissible police and intelligence behaviour beyond the limits of reasonable conjecture. This ambiguity is addressed and we make recommendations on the matter in Part V, Chapter 4 and Part X, Chapter 5.

(iii) Statutory barriers to obtaining information from sources with access to "private sector" records

74. By the expression "access to private sector records" we mean the obtaining, from a source who is not in the employ of a government institution, information which he possesses by reason either of a business or professional relationship with a third party. For example, a lawyer or doctor in private practice may have records or personal knowledge of discussions with clients or patients who may be of interest to a security intelligence agency or a police force. A manager of a financial institution (e.g. a bank or trust company) might also have access to financial data concerning individuals of interest.

75. Although we have heard no evidence concerning instances of R.C.M.P. access to private sector records, we have examined the R.C.M.P. submission to the Commission of Inquiry into the Confidentiality of Health Records in Ontario in June 1979. That submission identified a number of situations when the R.C.M.P. had approached private medical practitioners in order to obtain medical or biographical information. In the area of V.I.P. security, the submission noted that the R.C.M.P. had approached doctors some 147 times within the past 15 years in order to determine whether a given individual constituted a threat to the safety of a V.I.P. The R.C.M.P. has also, although less frequently, approached medical doctors and psychiatrists about the reliability of individuals, for security screening purposes. The submission noted that on two occasions R.C.M.P. officers approached medical doctors for information on prescriptions given to patients, in order to further drug investigations.

76. We have no data on the number of occasions, if any, on which the R.C.M.P. has approached other professionals to act as sources in providing access to private sector records, and therefore we cannot treat approaches to these other professionals as "past practices not authorized or provided for by law". Nonetheless, we raise the possibility of the violation of federal and provincial laws in obtaining access to private sector records because of the

potential problems to be encountered in this area. Similar problems have surfaced in the United States.

77. Federal restrictions on the use of sources with access to private sector records are few. One statute, the Telegraphs Act,[44] requires certain employees of private telegraph companies falling under federal jurisdiction to swear an oath of secrecy as to information they acquire in the course of their duties. Unauthorized disclosure is a summary conviction offence. Another example of federal controls on private sector information is the Canada Shipping Act,[45] which provides for the privacy and confidentiality of wireless messages sent to ships at sea. The penalty for wrongful disclosure may include a fine and imprisonment.

78. More likely to constitute barriers are provincial statutory restrictions on the disclosure of personal information obtained in the course of a professional or commercial relationship. We have reviewed provincial legislation governing the legal and medical professions in Quebec and Ontario as examples of such statutory provisions. These provisions serve as a general illustration of restrictions likely to be found in other provinces. In both Ontario and Quebec, the legislation we examined sets up a framework, *inter alia*, for regulating the conduct of professionals through a governing body.

79. In Ontario the Health Disciplines Act[46] and the regulations enacted pursuant to it define as professional misconduct a breach by a medical doctor of his obligation of confidentiality vis-à-vis his patients. Such conduct is punishable by a variety of disciplinary sanctions administered by the governing body. Exceptions to the general rule of confidentiality are very narrow and would not extend to most security intelligence agency or criminal investigations, nor would they permit release of a patient's psychiatric or medical files to enable authorities to cope with an emergency such as a terrorist attack or a hostage-taking incident. The severity of the confidentiality rule is mitigated by the fact not only that the disclosure must come to the attention of the Discipline Committee but that when it does the Committee is unlikely to discipline a doctor if the disclosure were made to avert a threat to human life.

80. The Law Society Act[47] of Ontario and the regulations and rules enacted pursuant to it make it a breach of that profession's code of professional conduct to disclose, except in limited circumstances, confidential information concerning a client. Breach of the code of conduct by a lawyer may result in disciplinary sanctions, including the loss of professional status.

81. In Quebec, lawyers, notaries and medical doctors fall under the authority of the Code des Professions,[48] as do some 35 other professional bodies, such as pharmacists, social workers and chartered accountants. Section 87 of the Code requires that the "bureau" of each professional corporation adopt in regula-

---

[44] R.S.C. 1970, ch.T-3.
[45] R.S.C. 1970, ch.S-9.
[46] S.O. 1974, ch.47.
[47] R.S.O. 1970, ch.238.
[48] 1978 L.R.Q., ch.C-26.

tions a Code of ethics which must include confidentiality provisions. The code also establishes disciplinary procedures, including the creation within each professional corporation of a discipline committee which handles all complaints lodged against its members for violations of codes of ethics. For example, a violation of the Règlement concernant le code de déontologie[49] adopted by the medical profession may result in disciplinary proceedings against doctors who divulge confidential information. Likewise, the Règlement concernant le code de déontologie,[50] adopted by the Bar, and the Loi sur le Notariat[51] impose confidentiality requirements for lawyers and notaries respectively. Finally, the Quebec Charter of Human Rights and Freedoms[52] makes provisions for professional secrecy, and provides only narrow exceptions, which again would not extend to police or security intelligence investigations. The Charter provides in section 49 that any unlawful interference with any right or freedom recognized by the Charter entitles the victim to obtain cessation of such interference and compensation for the moral or material prejudice resulting therefrom. In the case of an unlawful and intentional interference, the party guilty of the interference may be condemned to pay exemplary damages.

82. While we do not wish to forecast the application of the secrecy provisions in Quebec, we are concerned that professionals who act as sources in providing access to private sector records may risk discipline, fines and the possible loss of professional status. This of course is primarily a problem for the source himself, but R.C.M.P. members who conspire with the source to effect an unlawful purpose may be guilty as a party to the offence by virtue of abetting it (section 21) and of the Criminal Code offence of conspiracy (section 423(2)).

83. In addition to the specific statutory provisions governing various professions, examples of which we have seen in Ontario and Quebec, general statutory or regulatory restrictions at the provincial level may govern disclosure of information to disinterested third parties. One such example is the Ontario Consumer Reporting Act.[53] That Act seeks to regulate the collection and dissemination of consumer credit information. Its provisions would restrict the release of personal, financial and career information to a security intelligence agency or police force, although identifying information (name, address, place of employment) may be released. This Act penalizes both the source who improperly provides access to private sector records and the person who seeks to obtain the information. Members of the R.C.M.P. who conspire with the source to breach the confidentiality provisions may again be liable to criminal charges of conspiracy under section 423(2) of the Code or, if the offence is committed, may be a party to the offence by virtue of having abetted it (section 21).

---

[49] Reg. 816-80, 20 mai 1980.
[50] Reg. 77-250, 5 mai 1977.
[51] L.R.Q. 1978, ch.N-2.
[52] S.Q. 1975, ch.6.
[53] S.O. 1973, ch.97.

in Canada to "turn" — i.e. to defect, or to remain in place as an agent of the Canadian Security Service — the member would thereby be guilty of an offence under section 63 of the Criminal Code. That section provides as follows:

> 63. (1) Every one who wilfully
>
> (a) interferes with, impairs or influences the loyalty or discipline of a member of a force,
>
> (b) publishes, edits, issues, circulates or distributes a writing that advises, counsels or urges insubordination, disloyalty, mutiny or refusal of duty by a member of a force, or
>
> (c) advises, counsels, urges or in any manner causes insubordination, disloyalty, mutiny or refusal of duty by a member of a force,
>
> is guilty of an indictable offence and is liable to imprisonment for five years.
>
> (2) In this section, "member of a force" means a member of
>
> (a) the Canadian Forces, or
>
> (b) the naval, army or air forces of a state other than Canada that are lawfully present in Canada.[54]

The section was introduced into Canada in 1953, one year after the passage of the Visiting Forces (British Commonwealth) Act and the Visiting Forces (North Atlantic Treaty) Act.[55] It may be inferred that the Parliamentary intent was to provide the same penalty for subversion of such forces as was applicable to subversion of members of the Canadian Forces. Whether that is a necessary inference or not, it is noted that the section defines "member of a force" as "a member of... forces of a state... that are lawfully present in Canada". While a military attaché may be lawfully present in Canada, he cannot be said to be a member of "forces" present in Canada. If the military intelligence officer is not a military attaché but is disguised in some non-military capacity in order to spy, he is not in Canada as "a member of a force" and, even though he holds a diplomatic visa, he may not be "lawfully" in Canada if he is engaged in espionage. Alternatively, whether the military intelligence officer is an attaché or described as a chauffeur, the fact that he holds a diplomatic visa is probably conclusive that he is present in Canada as a diplomat and not as a member of a military force. For these reasons, we conclude that the factual situation envisaged does not give rise to the commission of an offence under section 63.

(f) *Removal of property of others and its delivery to the police*

85. Undercover operatives, as well as supplying intelligence as a result of their personal observations, have removed documents of intelligence interest from a targetted organization. The classic example is that of Mr. Igor

[54] 1953-54, ch.51, s.63.

[55] S.C. 1952, chs.283 and 289.

Gouzenko who, in September 1945, defected from the Soviet Embassy in Ottawa with documentary evidence of Soviet espionage in Canada and the United States. Based on what Mr. Gouzenko told the police, the documents he brought with him and subsequent investigations, the R.C.M.P. pieced together the espionage roles of some officials of the Soviet Embassy and a number of other individuals. Yet witnesses before us have asked whether the removal of documents in circumstances such as Mr. Gouzenko's may amount to the offence of theft, contrary to section 283 of the Criminal Code, and whether the receipt and retention of documents by the Security Service may constitute the offence of possession of property obtained by crime, contrary to section 312 (1). We do not intend to quote those sections, for we consider that the law of theft and of possession of stolen property does not impede the receipt and retention of documents defectors are likely to bring with them and which relate to the statutory mandate which we shall be recommending for the security intelligence agency. Any such documents are likely to relate to the commission of crime, and in our view the removal and retention of such documents by the defector or members of the security intelligence agency would not be a crime, if the information is disclosed to the appropriate law enforcement authority.

86. We recognize that there may be cases in which a defector brings documents to the security intelligence agency and those documents are neither evidence of a crime nor do their contents fall within the purview of the agency's mandate. We do not consider that such a situation requires any change in the law. Rather, we think that it should be handled in accordance with the proposals which we have developed with respect to the dealings between the federal and provincial attorneys general when evidence that violations of the law, may have been committed by a member or agent of the security intelligence agency. Our proposal in that regard is found in Part V, Chapter 8.

(g) *Civil wrongs*

87. A further issue of concern in both the Security Service and the C.I.B. is the commission of intentional civil wrongs by undercover operatives. While not involving a violation of federal, provincial or municipal law, civil wrongs merit consideration as an issue since they constitute an interference with personal rights to which society attaches significance and which the common and civil law therefore consider worthy of protection.

88. The range of potential civil wrongs arising from the use of undercover operatives is both broad and difficult to predict. Two acts in particular — inducing breach of contract and invasion of privacy — have been brought to our attention. We deal with these here.

89. The Force may have sought to obtain information from individuals such as bank managers whose positions impose upon them an express or implied duty in contract to keep in confidence information which they receive in that position. In such cases, the individuals may be civilly liable for breach of contract. R.C.M.P. members who procure such breaches of contract may be liable in tort for inducing breach of contract. One textbook states that liability for interference with contractual relations of this sort will attach if the intervenor

with knowledge of the contract and intent to prevent or hinder its performance, either,

(1) persuades, induces or procures one of the contracting parties not to perform his obligations, or

(2) commits some act, wrongful in itself, which prevents such performance.[56]

There appear to be two principal means in the situation noted above by which liability for inducing breach of contract may have been avoided. A leading text states:

> A distinction is sometimes drawn between persuasion, inducement or procurement, on the one hand, and advice on the other: the former being actionable, but not the latter...[57]

No liability attaches for simply advising an individual to breach his contract. It seems unlikely, however, that the means employed by the Security Service to "persuade" a person to breach his contract would be viewed as mere "advice".

90. The second and more likely means of avoiding liability for inducing breach of contract lies in the defence of justification. The same text notes:

> While spite or an improper motive on the part of the defendant is not an essential part of the plaintiff's cause of action, the purpose prompting his conduct may, on the other hand, be so meritorious as to require sacrifice of the plaintiff's claim to freedom from interference... The issue in each case being... whether, upon a consideration of the relative significance of all the factors involved, the defendant's conduct should be tolerated despite its detrimental effect on the interests of the other. For this purpose, it has been said, the most relevant are the nature of the contract, the position of the parties to it, grounds for the breach, the means employed to procure it, the relation of the person procuring it to the contract-breaker, and the object of the person procuring the breach. Thus, it seems clear that if the methods of interference are in themselves unlawful, at any rate where a fraud or physical violence is employed, there can be no justification, even if the defendant would have been privileged to accomplish the same results by proper means....
>
> In several cases, a privilege to protect the public interest has been recognized, as where the defendant acted for the sake of upholding public morality.[58]

While the Security Service (and indeed, the C.I.B., where such potential liability arises in the course of its undercover operations) may not be protecting public morality, there is a compelling argument that inducing an individual to provide information for intelligence reasons in breach of his contract can be justified on grounds of public interest.

---

[56] Fleming, *The Law of Torts*, Sydney, The Law Book Company, 1977, (5th ed.), at p. 678.

[57] *Ibid.*, at p. 679.

[58] *Ibid.*, at pp. 682-3.

91. The second possible civil wrong we examine here is that which the same textbook states

> . . . is often compendiously called the 'right of privacy'. In its broadest sense, the interest involved is that of 'being left alone', of sheltering one's private life from the degrading effects of intrusion or exposure to public view.[59]

The text notes that the right to privacy has not, at least under that name, received explicit recognition by British courts. Another text also lists infringement of privacy as a "doubtful tort".

> The balance of such authority as there is, appears to be clearly against the existence of any independent tort of invasion of privacy...[60]

It is not clear in Canada whether an independent tort of invasion of privacy exists. In *Motherwell* v. *Motherwell*[61] the plaintiff succeeded in an action for breach of the right of privacy. In *Burnett* v. *The Queen in Right of Canada*,[62] the court held that it is not clear that there is no tort of invasion of privacy so that the action must proceed to trial on its merits. The court quoted from an earlier decision where it was said:

> It may be that the action is novel, but it has not been shown to me that the Court in this jurisdiction would not recognize a right of privacy. The plaintiff therefore has the right to be heard, to have the issue decided after trial.[63]

92. In the absence of a clear statement as to whether invasion of privacy is a tort, so that protection of the right of privacy is afforded as it is by privacy legislation enacted in some provinces, we must consider other bases for the potential right of action. The tort of trespass would not afford such a basis, since its boundaries are defined in relation to the plaintiff's person and property, and are not drawn in relation to a broader right to be left alone. Even the tort of nuisance offers only modest support; for the tort to occur, the offensive conduct must be devoid of any social utility and directed solely at causing annoyance. It is unlikely that the use of undercover operatives for a legitimate criminal investigative purpose or in order to fulfill the mandate of the Security Service can be regarded as an activity devoid of social utility. Therefore, in light of the uncertainty surrounding the existence or scope of the tort of invasion of privacy, and the probable inapplicability of trespass and nuisance to typical undercover operatives, we do not consider that these torts pose a real legal problem in undercover operations, at least so long as such operations are carried out within the mandate of the respective branches of the Force.

---

[59] *Ibid.*, p. 590.
[60] *Winfield and Jolowicz on Tort*, (10th ed.), at p. 492.
[61] (1976) 3 D.L.R. (3d) 62 (Alta. C.A.).
[62] (1979) 23 O.R. (2d) 109 (Ont. H.C.).
[63] *Krouse* v. *Chrysler of Canada* [1970] 3 O.R. 135 at 136.

C. NEED AND RECOMMENDATIONS — BRIEF SUMMARY

93. There can be no doubt about the continued need to use undercover operatives both for criminal investigation and security intelligence work. When information is required about those who maintain a high degree of secrecy in carrying out criminal activities or activities threatening the security of Canada, often the use of undercover operatives is the only effective means of obtaining it. However, as our analysis of the legal difficulties involved in the use of undercover operatives has shown, very serious doubt exists as to whether operatives may be used by either the criminal investigation side or the security intelligence side of the R.C.M.P. without violating existing federal and provincial laws. Therefore, because we think the use of undercover operatives is necessary and because we believe that both police and security intelligence practices should be lawful, we will recommend a number of changes in the law to remove doubts about the reasonable use of operatives for both police and security purposes. We will make our detailed recommendations for changes relating to security intelligence operations in Part V, Chapter 4 and for changes relating to criminal investigations in Part X, Chapter 5.

94. One other legal issue which may arise in using undercover operatives is entrapment. Entrapment arises as a legal issue only in cases resulting in prosecution. Therefore, it will be dealt with primarily as a problem relating to the criminal investigations side of the Force. Although there is no offence of entrapment in the Criminal Code, many believe (a) that such an offence should be introduced into the Code, or (b) that a defence should be established for an accused person who committed a criminal act as a result of inducement by an undercover operative, or (c) that evidence obtained by entrapment should be excluded, or (d) some combination of the above. We will make our recommendations on this subject in Part X, Chapter 5.