# CHAPTER 4

# INFORMATION COLLECTION METHODS

**1.** Because of the secrecy maintained by those who pose the most serious threats to Canada's internal security, the security intelligence agency must be authorized to employ a variety of investigative techniques to enable it to collect information. The means available to it must range all the way from studying open sources of research material and obtaining information from citizens, police forces and government agencies (foreign and domestic) to using much more covert and intrusive methods that may involve the use of powers not available under law to the ordinary citizen. In this chapter we review this wide range of intelligence collection techniques and make recommendations as to which should be available under law to the security intelligence agency and what controls should govern their use.

## A. BASIC PRINCIPLES

**2.** The proposals set forth in this chapter on methods of investigation and their control are based on five fundamental principles which we think it important to state at the outset. They should underlie whatever system of powers and controls may be used for intelligence-gathering in the future:

(a) The rule of law must be observed. We have insisted upon adherence to the rule of law at several points earlier in this Report and we re-emphasize it here. No technique of intelligence collection should be employed which entails the violation of criminal law, other statutory law or civil law (federal, provincial or municipal). If for national security purposes it is considered essential that the security intelligence agency use an investigative technique which involves the violation of law, then those responsible for enacting laws — federal, provincial or municipal — must be persuaded to change the law so that the use of the technique by the security intelligence agency is made lawful.

(b) The investigative means used must be proportionate to the gravity of the threat posed and the probability of its occurrence. In a liberal society, which as a matter of principle wishes to minimize the intrusion of secret state agencies into the private lives of its citizens and into the affairs of its political organizations and private institutions, techniques of investigation that penetrate areas of privacy should be used only when justified by the severity and imminence of the threat to national security. This principle is particularly important when groups may be subjected to security intelligence investigations although there is no evidence that they are about to commit, or have committed, a criminal offence.

(c) The need to use various investigative techniques must be weighed against possible damage to civil liberties or to valuable social institutions. The indiscriminate use of certain techniques of investigation by a security intelligence agency, even though lawful, may do great damage to the fabric of our liberal democracy. Spying on political organizations which are critical of the status quo can have a chilling effect on freedom of association and political dissent. Similarly, the widespread, indiscriminate use as informants, of journalists, trade unionists, and professors, can do grave damage to the effective functioning of a free press, free collective bargaining, and freedom of intellectual inquiry.

(d) The more intrusive the technique, the higher the authority that should be required to approve its use. The authorizing of security intelligence officers to use various techniques of information collection must be carefully structured. The least intrusive techniques should not require any prior approval by senior authorities, but as the investigation of a group or individual intensifies, the use of more covert and intrusive techniques should require the approval of more senior officials. At the other end of the spectrum, where the most intrusive techniques of all are involved, the approval of authorities external to the agency itself should be required. Where the agency is authorized by statute under strictly defined conditions to use extraordinary techniques of investigation which would be a criminal offence if used by an ordinary citizen, the judiciary should make the authoritative determination as to whether the statutory conditions have been met.

(e) Except in emergency circumstances, the least intrusive techniques of information collection must be used before more intrusive techniques. Situations may arise in which the only opportunity for obtaining information on a subject is through the application of one or more relatively intrusive techniques. But the normal rule should be to use the least intrusive techniques first.

## B. CONTROLLING THE LEVEL OF INVESTIGATION

**3.** In 1977 the R.C.M.P. began to develop a new system for establishing more control at the Headquarters level over Security Service investigations. The key element in this control system was the Operational Priorities Review Committee (O.P.R.C.), a committee of senior Security Service officials, and a lawyer from the Department of Justice assigned to the R.C.M.P. The terms of reference of this Committee were finally approved by the Commissioner of the R.C.M.P. in 1979.[1] This system of controlling security intelligence investiga-

---

[1] Commissioner Simmonds referred to the role of this Committee in his statements to the House of Commons Committee on Justice and Legal Affairs at *in camera* meetings of the Committee on November 24 and November 29, 1977. The O.P.R.C.'s terms of reference are classified Secret. References to the role of the Committee can be found in volumes of the record of the Commission's public hearings, e.g. in Vols. 127, 138 and 163.

tions had much in common with a system of controlling the F.B.I.'s domestic security investigations introduced by the Attorney General of the United States, Edward Levi, in 1976.[2]

**4.** The F.B.I. system incorporates a four-fold classification of information collection activities. First, maximum discretion is permitted at the field or desk level in the collection of information from open sources or the receiving of reports from public authorities or private citizens. At the next level, the system permits active security investigations to be launched at the field level and carried on for a limited period of time (90 days) using relatively less intrusive techniques with no higher approval than that of the senior officer in a particular regional office. The purpose of such a 'preliminary investigation' is to see if there is sufficient evidence to justify a full-scale investigation using more intrusive techniques. The extension of the level of investigation beyond 90 days, requires Headquarters approval. At the third level are 'limited investigations' involving the use of more intrusive techniques such as full-scale physical surveillance and interviewing but not the full range of intelligence collection. Investigations at this third level require the approval by the Special Agent in Charge or F.B.I. Headquarters. Finally, the level of 'full' investigation involves the use of all legally available techniques, including undercover agents and the interception of private communications. The F.B.I. requires Headquarters approval for full investigations. In the F.B.I. system, the Attorney General or his designate must be notified when full investigations are approved, and may terminate a full investigation at any time; the extension of a full investigation beyond a year requires the written approval of the Department of Justice.

**5.** We think that an acceptable system for controlling information collection by a security intelligence agency should distinguish three basic levels of investigation: the first leaves discretion at the field or desk level without requiring approval by senior management at Headquarters; the second requires approval by senior management of the agency; the third requires approval by the Minister responsible for the agency. The system we propose is based on this three-level approach.

---

[2] For an account of this system see John T. Elliff, *The Reform of F.B.I. Intelligence Operations*, Princeton, N.J., Princeton University Press, 1979. The "Levi Guidelines" are printed in Appendix I of this book. It is very important to note that this system of control does *not* apply to counter-espionage or counter-intelligence operations of the F.B.I. In December 1980, Attorney General Benjamin Civiletti issued guidelines entitled "The Attorney General's Guidelines on Criminal Investigations of Individuals and Organizations". These guidelines govern three types of investigations: general crimes investigations, racketing enterprises investigations and domestic security investigations. Part III, which covers domestic security investigations, reads as follows: "The Attorney General's Guidelines on Domestic Security Investigations [the "Levy Guidelines"] promulgated in 1976, shall continue to govern such investigations".

*Level One: Information collection and investigation requiring only field level approval*

**6.** We think there must be ways in which members of the security intelligence organization can collect information without being required to meet any exacting evidentiary standard or to obtain the approval of higher authorities. It would be unreasonable to require a security intelligence agency to have "reasonable and probable grounds" before it can collect information about any subject. It must start somewhere. For this reason we think it is incorrect to apply, as the 1975 Cabinet Directive does, the same evidentiary standard ("reasonable and probable grounds to believe" that an individual or group "may be engaged in or planning to engage in" an activity threatening the security of Canada) to all means of collecting information. The security intelligence agency should be authorized to initiate the collection of information both from open sources and through less intrusive techniques on a much more speculative basis. Requiring the same evidentiary standard for all kinds of information collection means either that the test will be ignored or that the agency will be deprived of the opportunity of gathering the basic information to determine whether or not it should employ the most intrusive investigative techniques.

**7.** At this level two types of information collection can be distinguished: information from open sources, and information of a more confidential kind which is the beginning of an investigation. The first kind of information includes public information from the news media, written publications, and attendance at public meetings. With the exception of opening files on individuals, the security intelligence agency should be able to collect and analyze information from any of these public sources so long as it relates to the agency's basic function of providing intelligence about threats to the security of Canada. The opening of files on individuals, even if the information comes from public sources, should conform to principles or guidelines. We shall elaborate on these shortly.

**8.** In the past the R.C.M.P. Security Service has not developed a sufficiently strong capacity to draw upon such public sources or to integrate such information with information obtained from covert sources. We think that it is essential for an effective security intelligence agency to develop a strong research capacity closely integrated with its investigative activities. The agency's research activities should provide understanding of the social, economic and political context, national and international, within which threats to Canada's internal security arise.

**9.** The collection of information from open sources should be directed by a planning process which reflects the intelligence priorities of the government. In Part VIII we shall propose ways in which the Cabinet and interdepartmental committees might improve their capacity to identify the government's intelligence requirements in all areas including security intelligence. The security intelligence agency should not be simply a passive recipient of these intelligence requirements. Through its monitoring of public sources of information it should alert the government to new sources of activity possibly threatening the

security of Canada, and it should be in a stronger position to analyze the extent to which certain political movements, in some quarters alleged to be subversive, are, on the contrary, contributing to the vitality and diversity of Canadian democracy.

**10.** The second kind of information which the members of a security intelligence agency should be able to collect at the field level without higher approval is information which can be obtained without applying intrusive techniques of investigation. Examples of sources of such information are:

- existing security intelligence agency records;
- interviews with the subject of investigation;
- information from other Canadian government agencies or police forces, but not information given by individuals or groups to the government on a confidential basis;
- information volunteered by, but not solicited from, private individuals.

The purpose of this low level, preliminary investigation is to ascertain whether there is sufficient evidence of conduct threatening the security of Canada to justify a more active and intrusive investigation. Investigative activity confined to these sources of information does not involve making inquiries about an individual in a manner which could damage the individual's reputation or interests. The information obtained from sources in government available at this stage should not include information which citizens have given to the government under conditions of confidence. We would also limit such information to that available from Canadian authorities because we think it important that information received from foreign intelligence agencies should be assessed at the Headquarters of the security intelligence agency before it is used by the agency in any way.

**11.** A further source of confidential information which might be available at this level of investigation is information received 'accidentally' through intrusive techniques which have been authorized for the investigation of another subject. The F.B.I. control system permits the use of existing human sources at this stage but not existing technical sources (i.e. electronic eavesdropping). We are dealing here with one aspect of the so-called 'spin-off' or accidental by-product phenomenon which will be discussed more fully in the next chapter. It is possible, for instance, that an authorized full investigation of organization A may yield information indicating that organization B may pose a serious threat to security, but a full investigation of organization B using intrusive techniques has not been authorized. In these circumstances, the system for controlling the use of intrusive investigative techniques could in effect be by-passed through exploiting this opportunity to use the incidental by-products of these techniques. Members of the agency at the field or desk level should be able to use this information in their preliminary appraisal of organization B but the use of information obtained in this way must be recorded at Headquarters, so as to facilitate the monitoring of the activity by the agency's senior management and by the independent review body.

**11A.** We think the surreptious trailing of individuals by the security intelligence organization is sufficiently intrusive that even when it is done for the limited purpose of "subject identification" if should be approved at Head-

quaters by a member who is at a higher level of responsibility than the most senior member in the field who is involved in the matter.

**12.** The F.B.I. system, as we have noted, requires that extensions of monitoring or preliminary investigations beyond 90 days be approved at Headquarters. We think that it is a sound practice, where confidential sources are being used, to require Headquarters approval for the continuation of a preliminary investigation of an individual or group beyond a set period of time. It is important that the senior management of the security organization continuously review the results of preliminary investigations to ensure that the investigative resources of the agency are properly and usefully deployed. The investigation of individuals and groups even at this low level of investigation should not be carried on indefinitely without reviewing the rationale for such investigations.

*Implications for opening and maintaining files*

**13.** There is a very widespread fear, both in Canada and in other western democracies, of the dangers to citizens which could result from the improper use of security files. Apprehension about the technical capability of the modern state to look into every nook and cranny of its citizens' lives and to retain, for unknown purposes, mountains of information about us all is reflected in the oft-heard phrase "they must have a file on me". Security intelligence agencies contribute to this apprehension: they can, and sometimes do, collect information about a very large number of individuals. The R.C.M.P. Security Services, maintains a name index which in December 1977 had 1,300,000 entries, representing 800,000 files on individuals. Access to computer technology greatly facilitates the ease with which information and opinions recorded in these files can be retrieved and correlated. Information or opinions which at the push of a button can be displayed or recorded on a computer print-out can just as readily be misused.

**14.** We believe that controls are needed to prevent a security intelligence agency from maintaining files on thousands of people who are not threats or potential threats to the security of Canada. To say that the agency can collect information regarding individuals as long as this information relates to the agency's mandate is so vague and loose a rule as to justify almost any collection programme. For example, as we shall describe in the chapter dealing with security screening for the Public Service (Part VII, Chapter 1), the Security Service has a long established programme for collecting information on individuals in Canada who are homosexuals. This programme is based on the premise that *some* homosexuals may be subject to blackmail should they come to occupy positions with access to security relevant information. As a second example, the Security Service has been known to open files on all Canadians who travelled to Soviet bloc countries. This and similar programmes involved the opening of files on many thousands of individuals who were not perceived as even possible threats to Canada's security. Such information collection programmes are far too indiscriminate and should never have been established.

**15.** A variety of controls — some governing the opening and review of files, others having to do with the reporting of information — are necessary. To prevent the establishment of such programmes in future we consider first the

question of opening a file. We believe that the security intelligence agency should establish general principles or guidelines as to when it is proper to open and maintain a file on a person. These guidelines should obviously not apply to opening files on individuals for purely administrative reasons. Thus, there should be no constraints on keeping files on agency employees or on various businessmen, consultants, or others who might be providing some administrative service to the agency. Nor should these guidelines apply to keeping files on the agency's human sources, whether voluntary or paid. With these exceptions, the security intelligence agency should open and maintain a file on a person only if at least one of the following three conditions is met:

(a) there is reason to suspect that the person has been, is, or will be engaged in activities which Parliament has defined as threats to Canada's security;

(b) there is reason to suspect that the person who is or who soon will be in a position with access to security classified information, may become subject to blackmail or may become indiscreet or dishonest in such a way as to endanger the security of Canada;

(c) the person is the subject of an investigation by the security intelligence agency for security screening purposes. (Once the investigation has been completed, the agency should not continue to add information to these files unless the information relates to category (a) or (b) above.)

**16.** All of these categories deserve further elaboration. Because the first category relates directly to the mandate of the security intelligence agency, there is little doubt in our minds that the agency should be allowed to collect information on individuals suspected of having a connection with a threat to security. The difficulty with this category lies in deciding what constitutes "suspicion" of a link or potential link to a security threat. For example, we believe that the agency should not collect information on all individuals who take holidays in the Soviet Union or who subscribe to a Communist newspaper. The link between such individuals and a threat to security is far too tenuous. On the other hand, it is appropriate for the agency to collect information on any individual who meets a suspected foreign intelligence officer in what appears to be a clandestine manner. The definition of suspicion may also vary depending upon the individual's position. Thus, the security intelligence agency should not collect information about a public servant whose function does not require a security clearance and who is on friendly terms in an open manner with a Soviet bloc diplomat. But if, on the other hand, the public servant holds a position with access to security classified information, such a relationship, even on an open basis, could be of legitimate interest to the agency. While there are complexities involved in interpreting the standard of evidence to apply in this category, we should emphasize that it is a far less exacting standard than the one we shall propose shortly to justify the use of intrusive investigative techniques.

**17.** The second category would allow the agency to collect information on those individuals (including public servants and M.P.s) who hold or are about to hold a position with the federal government with access to security classified information and whose behaviour is such that they may become dishonest or

indiscreet or likely targets for blackmail in a manner which would endanger the security of Canada. As in the first category, there is the problem of what constitutes grounds for suspicion. Under what conditions, for example, is a person a likely target for blackmail? A second problem concerns whether or not this category is too narrow. Why should the agency not be allowed to collect information about illicit behaviour on the part of individuals who *might* in future hold a position with access to security relevant information? We acknowledge the risk in preventing the agency from collecting information on such individuals. There is little doubt that some of this information might be useful at some point in the future. But we believe that the risk of abuse in collecting information on so broad a category of people — as demonstrated by the Security Service's long standing programme of collecting information on homosexuals — is far greater. The government would have no way of properly defining what the agency should and should not collect. The result would likely be a security intelligence agency which was intruding far too much into the lives of Canadians.

**18.** Under the third category, the agency would be allowed to retain information relating to an investigation it has undertaken in regard to a security screening case concerning immigration, citizenship, or employment in the Public Service. In conducting such an investigation, the agency may conclude that the information about the individual is not relevant to security. (It may, for example, investigate an allegation concerning an individual which turns out to be false.) Nevertheless, the agency should be allowed to retain such information because of the possibility of the same allegation recurring many years after the original security screening investigation. The agency, once it has opened such a file should not continue to feed information into it unless the information relates to the first two categories noted above.

**19.** In putting forward these principles to help determine when it is proper for the security intelligence agency to open and maintain files on individuals, we emphasize that these principles should not apply to groups, organizations or movements which relate to or provide a context for the agency's mandate. Thus, those within the agency should be allowed to collect material from public sources on a wide range of topics including significant political trends or movements. Some of this material will contain names of individuals — for example, a newspaper article on the likely development of a new political party in Canada. The agency should be able to keep such information so long as the names of, and information about, individuals referred to in the material are not fed into an information retrieval system, whether computerized or manual, which is used for operational or security screening purposes. The agency will obviously want to retrieve information about individuals from its administrative and source files or research files, but the storage and retrieval system which relates to that material, should be distinct from the one used when advising government about individuals whose activities relate directly to a security threat.

**20.** Another protection against misuse of the information should lie in the conditions under which information can be reported to those who have the power to use it in ways which may adversely affect individuals. The most

important area of concern should be the security screening process, which may result in an individual being adversely affected by a report from the security intelligence agency. To meet concerns in this area we recommend, in Part VII of the Report, the establishment of a Security Appeals Tribunal, empowered to review the case of any individual who suspects that he has been or or may have been adversely affected by an inaccurate or unfair report. Also, later in this part of the Report we make recommendations as to the conditions under which the security intelligence agency may report information to police or government authorities in Canada or abroad and recommendations that the agency be prohibited from disseminating information about individuals to the media or any non-governmental bodies, including private employers. An important function of the independent review body which we shall propose (the Advisory Council on Security and Intelligence) would be to audit security intelligence operations to ensure compliance with these reporting rules.

**21.** The senior management of the security intelligence agency should maintain a sound programme of file review to extract material which in no way relates to the agency's mandate, or is no longer of use, so that it can be destroyed. The R.C.M.P. Security Service has maintained such a programme in recent years. Between January 1972 and June 1977, for instance, while 501,000 new files were opened, 332,201 were destroyed. Of course, as the destruction of the files relating to Operation Checkmate indicates there is a potential for abuse in destroying as well as in opening files. We have encountered instances in which instructions have been given to destroy files in order to obliterate any record of questionable activities. File destruction should not be carried out in an *ad hoc* manner but according to a clearly established schedule and based on criteria approved by the Minister responsible for the agency.

*Level Two: Investigative activity requiring Headquarters approval but not ministerial approval*

**22.** An intermediate level of investigation, which does not employ the full range of investigative techniques available to the security intelligence agency but would go beyond the preliminary stage, involves the following:

- obtaining information from foreign agencies;
- the use of "undeveloped casual sources"[3] and interviews with persons about the subject of investigation;
- physical surveillance;
- confidential government biographical[4] information for the limited purpose of subject identification (subject to the limitations and controls we recommend later).

[3] For an explanation of this term see Part III, Chapter 9, and paragraph 62 of this chapter.

[4] For an explanation of the distinction between 'biographical' and 'personal' information see section H of this chapter.

Decisions to apply this more active and intrusive kind of investigation to a group, or to an individual who is not connected to a group which is already the subject of an approved investigation, should be made at the Headquarters level of the security intelligence agency. By Headquarters level we mean members at Headquarters who are at a higher level of responsibility than the most senior member in the field involved in the matter. Such decisions would normally be made as the result of a preliminary (level one) investigation and would have the objective of ascertaining whether there is sufficient evidence to justify a full investigation. Headquarters approval of an intermediate investigation should be for a limited time. We suggest a maximum of six months.

**23.** The composition of the body which approves decisions at Headquarters at this stage should be a matter for the Director General and his senior management to determine, but presumably the heads of the main operational branches would play a central role in the approval process. Decisions at this stage can lead to one of three possible courses of action: termination of the investigation, continuation of the intermediate level of investigation for another period of time, or application for authorization of a full investigation. These are important targetting decisions and it is essential that they be made after a careful review of investigative results by those in the organization best equipped to analyze the results and best able to make responsible policy decisions.

**24.** We realize that there should be considerable flexibility in determining which of the less intrusive techniques of investigation require Headquarters approval and which do not. Therefore we recommend that this matter be regulated by administrative guidelines rather than by statute. These guidelines should be developed by the security intelligence agency and approved by the Solicitor General. They should provide for emergency situations so that an intelligence officer in the field can take advantage of important investigative opportunities which would be lost if Headquarters approval was required. But the guidelines should provide that, in such situations, Headquarters be notified as soon as possible and not later than 48 hours after the use of the technique.

**25.** While the security intelligence agency's use of the methods of collecting information available to it in level one and level two investigations would not require approval outside the agency itself, there should be an effective system of *ex post facto* review of investigative activities at these levels. This system of review should involve persons outside the agency itself and should include at least the following:

(a) regular checks and audits by the independent review body (the Advisory Council on Security and Intelligence);

(b) periodic reports about the extent and distribution of activity at these levels to the Deputy Solicitor General and Solicitor General;

(c) a report of the extent and distribution of activity at these levels, at least annually, to the Cabinet Committee on Security and Intelligence and to the Parliamentary Committee on Security and Intelligence.

*Level Three: Investigative activity requiring approval by the Minister, and in some cases authorization by a judge*

**26.** Beyond the first two levels of investigation are what might be termed full investigations. These are investigations which employ any of the following methods:

(a) undercover members, human sources (beyond "undeveloped casual sources");

(b) electronic surveillance (telecommunications intercepts, planting of hidden microphones, intrusive visual surveillance by electronic means and use of dial digit recorders);

(c) surreptitious entry to search or seize (for purposes other than electronic surveillance);

(d) mail checks (examination of mail covers and opening mail);

(e) access to confidential personal information about individuals or groups held by governments or private sources.

These techniques should be used by the security intelligence agency only to the extent authorized by law. Later in this chapter we shall recommend changes in the law to make these techniques available to the agency under proper conditions and controls.

**27.** We believe that decisions to subject an individual or the members of an organization to any of the techniques listed above are so important, in terms of both the effective deployment of the security agency's resources and the potential impact on civil liberties, that they should be based on evidence that meets a standard defined by statute. Except in emergency circumstances, such decisions should be approved by the Solicitor General, as the Minister responsible for the agency. We should make it clear that the decisions we refer to here are ones that determine that evidence obtained through less intrusive techniques of investigation justifies intensifying the general level of investigation to the most intrusive stage. Particular techniques of investigation may require an additional level of authorization. For instance, under our recommendation the use of electronic surveillance, surreptitious entry or a mail check, or access to certain kinds of confidential information, would require judicial authorization.

**28.** The procedure we envisage for initiating a full investigation of an individual or group would involve three stages:

Stage 1: Approval by a committee including senior management of the security intelligence agency, and representatives of the Department of Justice and the Minister responsible for the agency.

Stage 2: Approval by the Solicitor General.

Stage 3: If the law requires a judicial warrant for the use of a technique (e.g. electronic surveillance), authorization of the use of that technique by a judge.

**29.** A procedure for emergency situations should be provided for. It should be possible for the Director General (or a person authorized in writing by the

Director General to act in his place) to initiate a full investigation for 48 hours, without obtaining Stage 1 or Stage 2 approval. However, the Solicitor General's approval should have to be obtained within 48 hours. If it is not obtained, the full investigation should have to be terminated. It is understood that, if the Solicitor General is absent or otherwise incapacitated, the Acting Solicitor General would be able to act in his place. The Director General should report immediately to the Minister each emergency authorization which he grants. This emergency procedure does not remove the necessity to obtain a warrant authorizing those intrusive techniques which later in this chapter we recommend require a judge's warrant.

**30.** The Committee at Stage 1 should include higher echelon personnel and be broader in the interests it represents than is now the case with the Security Service's Operational Priorities Review Committee. We think the Committee should normally include the Director General of the agency. If he cannot attend, he should be informed as soon as possible if the Committee approves the initiation of a full investigation, for no such proposal should go forward for ministerial approval unless it is supported by the Director General. The senior legal adviser from the Department of Justice, whose position is fully described in Part VI of this Report, should also be a member of the Committee. His particular role should be to consider whether the proposed target of a full investigation is within the statutory mandate of the agency and whether the statutory standard for a full investigation has been met. The Committee should also include a senior official from the Department of the Solicitor General to ensure that a member of the Minister's staff who is not a member of the agency is fully apprised of the factors which entered into the decision to launch an intensive investigation. We think that the Assistant Deputy Solicitor General who heads the Police and Security Branch in the Solicitor General's Department would be the most appropriate person to perform this function. The selection of the security intelligence officers for this Committee should be left to the discretion of the Director General and his senior management team. The main considerations should be the inclusion of members with operational expertise in the area of investigation concerned and of senior officers with policy-making responsibilities.

**31.** The Committee which reviews proposals for the initiation of full investigations should not reach its decisions by majority vote. As we have stated above, no proposal to open a full investigation should be presented for ministerial approval without the Director General's support. Moreover, if the legal adviser believes that the subject of a proposed full investigation lies outside the statutory mandate of the security agency and he is unable to persuade the Committee of this, the question of its legality should be resolved by the Deputy Attorney General. On the other hand, if the representative of the Solicitor General's Department opposes a full investigation which the Director General and his colleagues believe should be undertaken and to which the legal adviser makes no objection, the Director General should put the proposal to the Minister. The security intelligence agency should also consult the Department of External Affairs before initiating a full investigation

involving the use in Canada of certain investigative techniques directed at a foreign government or a foreign national in Canada.

**32.** The ministerial approval called for in this procedure would entail a major extension of direct ministerial involvement in controlling security intelligence operations. At present under section 16 of the Official Secrets Act the use of electronic surveillance for national security purposes requires the authorization of the Solicitor General. There were some who questioned this requirement when it was introduced in 1974 on the grounds that it involved a Minister to an inappropriate degree in the day-to-day operations of the Security Service. How can we now justify expanding the scope of ministerial approval for security intelligence investigations? Our justification for doing so is based on a number of related points. We believe that in a system of responsible government, responsible Ministers should be accountable for the policies of the security intelligence agency. Further, our examination of Security Service activity has led us to the conclusion that many of the most important policy decisions relative to the work of a security intelligence agency arise in the process of assessing the degree of security threat and necessary countermeasures in individual cases. A number of investigative techniques have a great potential for invading privacy and impinging on civil liberties. In this class are the planting of state-paid undercover agents in political organizations, as well as techniques that involve the exercise of extraordinary powers denied to ordinary citizens, such as electronic surveillance, the opening of mail, surreptitious entry and access to confidential information. The decision to subject an individual or group to any or all of these techniques for national security purposes is a decision with important policy implications which in our view ought to have the approval of a responsible Minister. Indeed, it is through his participation in these decisions that the Minister responsible for a security intelligence agency is most likely to have the 'window' he needs into the agency's activities.

**33.** Our proposals also include a check on ministerial power by requiring judicial authorization of warrants to exercise the extraordinary powers of electronic surveillance, surreptitious entry, mail checks and access to confidential government information. This proposal, it might be argued, suggests an unacceptable extension of judicial authority into decisions which should be reserved for responsible Ministers. We do not think so. Under our proposal, the judiciary's role would be to determine whether or not a statutory standard established by Parliament as a condition for exercising certain extraordinary powers has been satisfied by the facts of a particular case. In normal situations of public law, the judiciary is involved when the exercise of a power is challenged after the fact. However, because of the secrecy inherent in the exercise of investigative powers by the security intelligence agency this practice becomes unrealistic, because the person affected does not normally learn of the use of this power and therefore cannot challenge its validity. Therefore we shall recommend that judicial approval be sought as a prior condition to the use of these powers. As we see it, the ministerial role with respect to these powers is to make policy decisions. For example, the Minister must decide whether the activities of a certain country's diplomats are sufficiently suspect and dangerous to risk the diplomatic repercussions of possible exposure of security

intelligence surveillance, or whether the activities of a violence-prone group pose a sufficient threat to the country's democratic process to warrant deploying the full investigative resources of the security intelligence agency. It is primarily questions of this kind which the Solicitor General must consider in deciding whether to approve an application for a judicial warrant. He might refuse to authorize an application even though convinced that it met the statutory standard. The Solicitor General should by no means be indifferent as to whether the legal requirements were satisfied by a proposed application: on the contrary, he should not approve the application for a judicial warrant unless satisfied that the legal requirements have been met. However, our proposals give the judiciary, not the Minister (or his legal advisers), the final decision whether the law is being properly applied. In our view this would ensure the application of the rule of law to these aspects of security intelligence operations and does not depart from the appropriate distribution of responsibilities between Ministers and judges.

**34.** In the system we propose, at the same time that the Minister gives his *general* approval to a proposal to initiate a full investigation he may also approve a proposal to apply for a judicial warrant to use one or more *particular* techniques. He might, however, not be asked for such approval or might withhold it until other techniques not requiring a judicial warrant have been used.

**35.** We recognize that without some protective mechanism there is a danger in this system of ministerial control. A Minister's denial of a request to initiate a full investigation may be based on improper considerations such as the desire to protect personal friends or partisan political supporters. Because of the danger in this and other areas, we shall recommend that the Director General must have direct access to the Prime Minister when he believes that the security intelligence agency is subject to improper ministerial direction, and, in extreme circumstances when in his view his concern is not dealt with adequately by the Prime Minister, to the independent review body.

**36.** The approval of a full investigation should be subject to standards set out in the statute governing the security intelligence agency. The statute should provide that a full investigation may be undertaken if:

(a) there is evidence that makes it reasonable to believe that an individual or group is participating in an activity which falls within the first three categories of activity (i.e. espionage, foreign interference and political violence) described as threats to the security of Canada in the statutory mandate of the security intelligence agency; and

(b) the activity represents a present or probable threat to the security of Canada of sufficiently serious proportions to justify encroachments on individual privacy or actions which may adversely affect the exercise of human rights and fundamental freedoms recognized and declared in Part I of the Canadian Bill of Rights; and

(c) less intrusive techniques of investigation are unlikely to succeed, or have been tried and have been found to be inadequate to produce the information needed to conclude the investigation, or the urgency of the matter makes it impractical to use other investigative techniques.

**37.** Full investigations should be approved for a maximum of one year at a time. The extension of a full investigation beyond its authorized duration should be subject to an approval process similar to that required for the initiation of a full investigation. Granted that security investigations must by their very nature frequently be more long-term than criminal investigations, nevertheless individuals and groups should not be subjected to indefinite investigation by the state's security agency. That is why it is important to review carefully the results of a full investigation to determine whether useful information has been obtained from the techniques employed and whether there is a basis for extending the full investigation for a further period.

**38.** When the new system of controls comes into force it is extremely important that it be applied as quickly as possible to all existing Security Service investigations which employ the techniques covered by a full investigation. This would involve an assessment of the current investigative activity of the Security Service in the light of new standards established by Parliament. Such a review and assessment should be a top priority of the senior management of the new security intelligence agency and of the Solicitor General.

**39.** Besides the system of prior approval for full investigations recommended above, there should be a system of *ex post facto* review of full investigations. This system of review should have at least the following elements:

(a) regular checks and audits by the independent review body (i.e. the Advisory Council on Security and Intelligence);

(b) a report at least annually to the Cabinet Committee on Security and Intelligence and to the Parliamentary Committee on Security and Intelligence of the range of full investigations and methods used.

**WE RECOMMEND THAT a system for controlling the collection of information by the security intelligence agency be established which distinguishes three levels of investigation.**

(7)

**WE RECOMMEND THAT investigations at the first two levels be regulated by administrative guidelines developed by the security intelligence agency and approved by the Solicitor General.**

(8)

**WE RECOMMEND THAT the statute governing the security intelligence agency require ministerial approval for full investigations, indicate the techniques of collection that may be used in a full investigation and stipulate that a full investigation be undertaken only if**

**(a) there is evidence that makes it reasonable to believe that an individual or group is participating in an activity which falls within categories of activities (a) to (c) identified, in the statute governing the security intelligence agency, as threats to the security of Canada; and**

**(b) the activity represents a present or probable threat to the security of Canada of sufficiently serious proportions to justify encroachments on individual privacy or actions which may adversely affect the exercise of human rights and fundamental freedoms as recognized and declared in Part I of the Canadian Bill of Rights; and**

(c) less intrusive techniques of investigation are unlikely to succeed, or have been tried and have been found to be inadequate to produce the information needed to conclude the investigation, or the urgency of the matter makes it impractical to use other investigative techniques.

(9)

WE RECOMMEND THAT the security intelligence agency and the Solicitor General should move as quickly as possible to apply this system of controls to all security intelligence investigations which are under way at the time this new system of controls is introduced.

(10)

WE RECOMMEND THAT, with the exception of administrative and source files, the security intelligence agency open and maintain a file on a person only if at least one of the following three conditions is met:

(a) there is reason to suspect that the person has been, is, or will be, engaged in activities which Parliament has defined as threats to Canada's security;

(b) there is reason to suspect that the person, who is, or who soon will be, in a position with access to security classified information, may become subject to blackmail or may become indiscreet or dishonest in such a way as to endanger the security of Canada;

(c) the person is the subject of any investigation by the security intelligence agency for security screening purposes. (Once the investigation has been completed, the agency should not continue to add information to these files unless the information relates to category (a) or (b) above.)

(11)

WE RECOMMEND THAT the security intelligence agency and the independent review body (the Advisory Council on Security and Intelligence) develop programmes for reviewing agency files on a regular basis to ensure compliance with the general principles for opening and maintaining files on individuals.

(12)

WE RECOMMEND THAT the storage and retrieval system for information on individuals whose activities are relevant to the security intelligence agency's mandate be separate from those systems pertaining to administrative, source and research files.

(13)

WE RECOMMEND THAT the security intelligence agency's files, documents, tapes and other matter be erased or destroyed only according to conditions and criteria set down in guidelines approved by the Solicitor General.

(14)

WE RECOMMEND THAT the security intelligence agency consult the Department of External Affairs before initiating a full investigation involving the use in Canada of certain investigative techniques directed at a foreign government or a foreign national in Canada.

(15)

**40.** The foregoing section of this chapter has dealt with the *general* system of controlling the collection of information by the security intelligence agency. It was designed to encompass the use of all techniques, without regard to their special legality. We now turn to those specific techniques which at present raise legal difficulties and which, therefore, may require changes in the law. The groundwork for this part of the chapter was laid in Part III where we analyzed the legal issues raised by the investigative methods used by the R.C.M.P. Security Service and indicated whether we thought that continued use of the method in the future was justified. In what follows we now set out the details of the legal and policy changes which we think should be made with respect to particular investigative techniques employed by a security intelligence agency.

## C. PHYSICAL SURVEILLANCE

**41.** Physical surveillance techniques are used to collect information about the movements, habits and contacts of persons by surreptitiously following them or observing their premises. In Part III, Chapter 8 we described how this technique had been developed by the R.C.M.P. Security Service and the general importance of physical surveillance operations, carried out to a large extent in the Security Service by the highly specialized Watcher Service. There is no doubt in our minds that expert physical surveillance must continue in the future to be an investigative technique available to Canada's security intelligence agency.

**42.** Much physical surveillance of a person's public movements and contacts is less intrusive than intercepting private communications or planting an undercover agent within an organization and should, whenever appropriate, be used before or instead of resorting to those more intrusive techniques. Still, we regard physical surveillance, whether for the limited purpose of identification or for other investigative purposes, as sufficiently intrusive to justify requiring approval at Headquarters (level two). When publicly financed surveillance teams, fully equipped and expertly trained, are directed to follow a person surreptitiously, noting every movement and contact, there should be reasonable grounds for believing that such a person, whether a citizen, a visitor or a diplomat, poses a threat, even unwittingly, to national security.

**43.** We think it would be wise, whenever practicable, for the security intelligence agency to continue to use specialized teams, such as the Watcher Service, for physical surveillance operations. Not only are such teams most likely to have the skill necessary to overcome the security measures employed by 'hard' targets in the espionage and terrorist fields, but also they can be better trained to minimize the risk of traffic accidents and other hazards associated with physical surveillance work. In locations where it is not feasible to use specialized teams, individuals who might be called upon to engage in surveillance work should continue to receive the most thorough training possible.

**44.** But more than a high standard of training and the maintenance of specialized teams will be needed if physical surveillance is to be carried on in the future on a satisfactory basis by our security intelligence agency. As we reported in Part III, Chapter 8, physical surveillance for both security and regular police investigations is very likely to involve a number of legal violations. At the conclusion of that chapter we took the position that, even though the legal violations resulting from physical surveillance operations may often be regarded as "minor infractions" or "technical breaches" of "merely regulatory laws", the continuation of physical surveillance without any changes in the law endangers the rule of law, for it implies that our security agency or police forces may in their institutional practices pick and choose the laws which they will obey. We argued that to permit a national police force or security intelligence agency to adopt a policy which entails systematic violations of "minor" laws puts these organizations at the top of a slippery slope and therefore that changes should be made in the law so that physical surveillance may be carried on without jeopardizing the rule of law.

**45.** A possible alternative to legal amendments is the establishment of a policy by attorneys general of not prosecuting surveillance team members who contravene legislation in the course of their duties. We reject this alternative. Such a policy would do nothing to resolve the dilemma of a government agency maintaining a practice that systematically involves the commission of illegal acts. Furthermore, a firm policy of non-prosecution might be rejected by the courts as an improper fettering of the attorney general's prosecutorial discretion. Thus we think the only proper alternative is to make appropriate changes in the relevant laws.

**46.** As was explained in Part III the laws which present difficulties in physical surveillance operations fall broadly into three categories: "rules of the road", the identification of persons and property, and trespass. Many of the laws which are apt to be violated in these areas are provincial statutes or municipal by-laws. One possible approach to these legal difficulties would be the enactment of federal legislation to provide with respect to both federal and provincial laws either a defence in defined circumstances or a procedure for authorizing what otherwise would be proscribed. Such provisions could be included in the legislation establishing the security intelligence agency. This approach would have the advantage of immediately providing a uniform legislative scheme across the country. However, we have serious doubts about the constitutionality of such an approach. It is far from clear that 'national security' or 'the security of Canada' (or, for that matter, 'national policing') constitutes a distinct subject matter of legislation over which the federal parliament has an exclusive or paramount authority. Even if these legal doubts can be set aside, we question the wisdom of unilateral action at the federal level exempting a national security intelligence organization (or a national police force) from provincial legislation. We think that unilateral federal action of this kind would undermine the possibility of fostering the kind of federal-provincial co-operation which in our view is essential to an effective system of national security in the Canadian federation. Moreover, we think it likely that the legislative changes needed to reconcile physical surveillance activities with

the rule of law may be needed just as much by provincial or municipal police forces as by a national security intelligence agency. Therefore we recommend the enactment of legislation by the Parliament of Canada to deal with breaches of federal laws and that the provinces be asked to enact provincial legislation to deal with violations of provincial and municipal laws.

*The specific amendments*

(a) *Rules of the road*

**47.** In Part III, Chapter 8 we reported that no evidence was before us to suggest that Criminal Code offences relating to the operation of motor vehicles have been committed or need to be committed by those engaged in physical surveillance. Therefore our recommendations for specific legislative amendments in this area are confined to provincial driving offences and municipal by-law infractions.

**48.** We think that provincial driving offences are best dealt with by the enactment by provincial legislatures of a defence available to a defined class of persons. Peace officers (a term including the R.C.M.P., provincial and municipal police forces) would be within this class, as would any other person designated (according to the function he performs) by provincial attorneys general upon the advice of the federal Solicitor General. These designated persons should include members of a security intelligence agency who regularly perform surveillance functions or who may be called upon to perform such functions. This statutory defence should be available only where a breach of traffic legislation occurs in the course of the driver's otherwise lawful duties, and the driver acts reasonably in all the circumstances, with due regard for the safety of others. We believe that the inclusion of these conditions in the legislation is necessary to ensure that the defences are not too broad. Section 3(4) of the New Brunswick Police Act[5] provides the following defence:

> A member of the Royal Canadian Mounted Police or a member of a police force shall not be convicted of a violation of any Provincial Statute if it is made to appear to the judge before whom the complaint is heard that the person charged with the offence committed the offence for the purpose of obtaining evidence or in carrying out his lawful duties.

We consider that this formulation is too broad in its scope to be applied to a security intelligence agency. Moreover, it lacks any requirement of necessity or of reasonable conduct.

**49.** At the same time as the recommended defence is introduced, a mechanism should be put in place which will both protect the defined class of person from personal liability in the event of actionable damage to a third party and provide an aggrieved third party with a means of recovering compensation in a proper case. Such a mechanism would recognize that the object of the statutory defence is not to deny redress to an innocent individual. On the other hand, individuals carrying out surveillance responsibilities should not be personally

[5] New Brunswick Police Act, Stats. N.B. ch.P-9.2 (1977).

liable where damage ensues, caused by what would otherwise be a breach of statute, provided that they act reasonably in the discharge of their otherwise lawful duties and with due regard for the property and the safety of others. To attach personal liability to such individuals would be unfair. We therefore consider that the federal government should accept responsibility for compensation to aggrieved persons through the ordinary civil process in the courts or through an agency similar to provincial Criminal Injuries Compensation Boards. The secrecy of the surveillance operation could be maintained by the use of *in camera* hearings in either case. The quantum of damages should in any such case be determined with reference to the same principles which guide the civil courts in such matters.

**50.** Violations of municipal by-laws, primarily "non-moving" and pedestrian violations, should also be dealt with in the same manner as provincial driving offences by seeking provincial co-operation to amend Municipal Acts or other relevant legislation.

(b) *Laws governing the identification of persons and property*

**51.** Legislation in this field exists both at the federal and provincial level. Consequently, we recommend that both federal and provincial governments be involved in amending their respective enactments. We would suggest that a provision be added to relevant legislation to permit the Director General of the security intelligence agency, or a senior officer designated in writing by the Director General, to apply to the senior government official charged with the administration of an enactment (e.g. the Superintendent of Motor Vehicles in the case of highway traffic legislation) to obtain identification or registration documents that will enable a surveillance operation to remain covert. The application would be accompanied by a sworn statement that the documents are reasonably necessary for the operation. Such identification should be deemed to comply with the requirements of the statute in question. For example, a driver's licence which contains false information will nonetheless be deemed to be a valid driver's licence, if it is applied for and granted pursuant to this provision. In the provinces where they are necessary, provisions should also be enacted to ensure that it shall not be an offence for an individual in defined circumstances to hold two valid licences (e.g. one in the individual's true name, and one in an assumed name) or to sign a specially obtained licence with other than one's usual signature. A record of all applications for 'false documentation' permits should be kept for periodic examination by the Solicitor General of Canada and by the attorneys general or solicitors general of the provinces where such applications are made.

**52.** The requirement in some provinces that an individual register his proper name upon entering a hotel can, we think, be safely relaxed in order to permit members conducting surveillance to register under a false name in the course of an investigation. It is our understanding that these registration laws were originally intended to allow the police to keep track of transients and to ensure that guests would not defraud hotel owners. Neither of these objects is affected by permitting members conducting surveillance to register under false names. We feel that there is no need for prior authorization in this situation; a

statutory defence enacted at the provincial level is the appropriate mechanism. The defence should be available to peace officers and other persons designated by provincial attorneys general on the advice of the federal Solicitor General who register in a hotel using a false name and address if they do so in good faith and if the use of a false identity is necessary for the performance of their lawful duties.

**53.** The legislative schemes we recommend here will also remove the temptation on the part of members of the R.C.M.P. to resort to violations of the Criminal Code in order to obtain and use appropriate cover documentation. Thus, where surveillance team members are supplied with documentation through a legislated scheme, there will be no obtaining by a false pretence, contrary to section 319 of the Criminal Code. Also, there will no longer be a need for cover documentation to be manufactured by the R.C.M.P. themselves for individuals engaged in surveillance, and there will therefore be no violations of sections 324 and 326 of the Criminal Code, dealing with forging and uttering forged documents. Similarly, there will be no need for members to personate someone else at a qualifying examination in order to obtain appropriate documentation; this resolves the problem, potential or actual, raised by section 362 of the Criminal Code. In short, selective amendments at the provincial level to what some have termed "minor" or "regulatory" laws will, with respect to these matters, eliminate the potential for violation of criminal laws in order to protect the security of Canada.

(c) *Laws relating to trespass*

**54.** An initially attractive solution to the trespass issue seems to lie in asking the owner of the target's apartment building, for example, for permission to enter the premises to search for the target's car. If such consent to enter is obtained, no offence is committed. While most individuals likely will grant permission to enter if the circumstances are explained to them, a real danger exists that the person's knowledge might eventually compromise the secrecy of the surveillance operation.

**55.** If entry into buildings and onto land is to be permitted for physical surveillance teams, it is best done with the protection of legislation. We are satisfied that the balance between property rights and the need for effective security intelligence operations favours the amendment of trespass legislation to permit entry onto land or into buildings (other than a house, or in the case of an apartment building, inhabited rooms) in order, for example, to determine the presence of an individual or of his vehicle or to plant tracking devices on the vehicle. Amendments to legislation should apply to federal and provincial police forces, as we have recommended in the section of this chapter dealing with rules of the road.

**56.** The legislation should be framed to provide a defence to a petty trespass prosecution where the accused is a peace officer or a person designated by the provincial attorney general and was engaged at the time of the entry in the discharge of his otherwise lawful duties and acting with due regard for the property rights of the owner. Furthermore, the trespass should be reasonably

necessary in all the circumstances. While it is hard to conceive of circumstances in which damage would occur, civil remedies against the Crown for damage occasioned in the course of such entries should continue to exist, as in the case of damages arising from automobile accidents. Again, no liability should be imposed on individual surveillance team members where they act in a fashion that entitles them to rely on the proposed defence. The federal government should compensate those individuals who suffer damages as a result of a trespass by security intelligence surveillance team members. The quantum of compensation should be assessed on the same basis as is the practice in civil courts, whether or not the civil courts or some other tribunal hear the complaint.

**57.** The Criminal Code offences of mischief (section 387) and damage to property (section 388) remain a problem. Increasingly effective methods of counter-surveillance necessitate considerable ingenuity on the part of individuals engaged in surveillance. To this end, surveillance operations may involve placing objects on a target vehicle. We accept the need for the use of such techniques. Therefore, we must address the problems caused by these Criminal Code offences. The only practicable solution we see is the enactment of a defence that will protect designated individuals acting in the course of their otherwise lawful duties, if they do no more damage or interfere no more with the property than is reasonably necessary for the purposes of the operation. In any event, the damage or interference should not be such as to create any danger in the use of the property. Civil recovery should be permitted according to principles similar to those enumerated in respect of rules of the road and provincial trespass legislation. This defence seems at first very broad; its ambit can be restricted considerably by limiting the number of designated individuals permitted to engage in such conduct.

**WE RECOMMEND THAT, in order to make it possible for physical surveillance operations to be carried out effectively by a security intelligence agency, changes be made in federal statutes and the co-operation of the provinces be sought to make changes in provincial statutes as follows:**

**(1)** *Rules of the road*

**(a) A defence be included in provincial statutes governing rules of the road for peace officers and persons designated by the Attorney General of the Province on the advice of the Solicitor General of Canada ("designated individuals") if such persons act**

**(i) reasonably in all the circumstances,**

**(ii) with due regard for the property and personal safety of others, and**

**(iii) in the otherwise lawful discharge of their duties;**

**(b) a defence similar to that referred to in (1)(a) above be included in relevant provincial legislation which authorizes municipal traffic by-laws;**

**(c) there be enacted by each of the provinces and territories, a provision for the protection of peace officers and designated individuals, saving them harmless from personal liability in civil suits, if such persons act**

**(i) reasonably in all of the circumstances;**

(ii) with due regard for the property and personal safety of others; and,

(iii) in the otherwise lawful discharge of their duties;

(d) the Government of Canada compensate those persons who, but for recommendation (c) above would be entitled to recover damages in a civil suit brought against a federally engaged peace officer or designated individual in a cause of action arising by reason of acts done or omissions occurring in the course of the work of such peace officer or designated individual and on the principle that the quantum of compensation should be assessed on the same basis as is the practice in the civil courts.

(2) *False identification*

(a) Provincial highway traffic legislation regulating the licensing and identification of persons and property be amended to permit the Director General or designated member of the security intelligence agency (or a duly authorized member of a police force) to apply for false identification to the senior government official charged with the administration of the legislation. Provision be made to permit the documents related to the application to be sealed and not to be opened without court order. It is further recommended that such amendments be made as may be necessary to remove all statutory restrictions on the signing or holding of more than one piece of identification in each case;

(b) provincial hotel registration legislation be amended to make available a defence to peace officers and designated individuals who register in a hotel under a false name provided that

(i) they do so in good faith, and

(ii) the use of a false name is necessary for the performance of their otherwise lawful duties.

(3) *Trespass*

(a) Provincial petty trespass statutes be amended to make available a defence to peace officers and designated individuals who enter onto private property other than private dwelling-houses or inhabited units in multi-unit residences but including vehicles, providing that

(i) entry onto private property is reasonably necessary in the circumstances;

(ii) they show due regard for the property rights of the owner; and,

(iii) they act in the otherwise lawful discharge of their duties.

(b) sections 387(1)(a) and 387(1)(c) and 388(1) of the Criminal Code be amended to make available a defence to peace officers and designated individuals in order to allow the attachment of tracking devices to vehicles, in order to assist in physical surveillance operations, provided that such persons

(i) act in the course of their otherwise lawful duties,

(ii) do no more damage or interference with the property than is reasonably necessary for the purposes of the operation; in any event, the damage or interference must not render the use of the property dangerous;

(c) civil remedies be preserved for both trespass and the affixing of devices in a manner similar to that recommended in respect of rules of the road. (16)

## D. UNDERCOVER OPERATIVES

**58.** The use of human sources and undercover members, collectively referred to by us as "undercover operatives", is the most established method of collecting information about threats to security. Despite the technological revolution which has provided a variety of technical alternatives as a means of penetrating secretive organizations, the undercover operative is likely to remain an extremely important source of information to a security intelligence agency.

**59.** An undercover operative can be a much more penetrating means of collecting information than any technical device. A technical source — whether a hidden microphone, a telephone tap, or a long-distance viewing device — is essentially a passive instrument which can record only what is said or done at one particular place. In contrast, undercover operatives — human spies — have frequently penetrated the innermost circles of groups, probed the intentions of their leading members, and actively attempted to thwart the groups by supplying misleading information, sowing the seeds of distrust amongst their members, or otherwise disrupting the groups.

**60.** While there is no doubt that undercover operatives have certain advantages as sources of information, there is also no doubt that the use of these individuals by a security intelligence agency involves a number of serious hazards. Unlike information obtained from the mechanical recording of conversations, information, particularly from human sources (who, it will be recalled, are not members of the Force) must be carefully assessed for its reliability. Mechanical recording devices do not lie or exaggerate or distort; human sources can and do. The use of undercover operatives also involves the security agency in directing individuals to deceive, indeed to betray, the organizations which they penetrate. Frequent participation in the planning and execution of deceitful and treacherous acts may have deleterious effects on the moral character of the 'handlers' of these operatives and the operatives themselves. Undercover operatives may go far beyond gathering information. They might endeavour to trap the group into carrying out incriminating actions — become, in effect, *agents provocateurs* — or carry out the kinds of disruptive tactics which have come under review by us. The agency which uses undercover operatives is apt to incur serious and difficult responsibilities to protect these individuals when they are exposed or have otherwise completed their assignment.[6] Also, there are, as we indicated in Chapter 9 of Part III, a number of laws which have been violated by the use of undercover operatives.

*The need for controls*

**61.** In the past, there has been far too little attention paid to the policy and legal problems associated with the use of undercover operatives in security

[6] For an examination of the policy issues arising from the use of informants in national security investigations see the following: Christopher Felix, *A Short Course In The Secret War*, New York, E.P. Dutton, 1963, esp. Ch. III; Garry T. Marx, "Thoughts on a Neglected Category of Social Movement Participant; the Agent Provocateur and the Informant", *American Journal of Sociology*, Sept. 1974, pp. 402-442; Geoffrey Robertson, *Reluctant Judas*, London, Temple Smith, 1976.

intelligence (or, for that matter, in criminal) investigations. This is particularly true of responsible Ministers. Guidelines concerning the use of undercover operatives were developed by the Security Service but were not submitted to, nor requested to be seen by, Solicitors General. Mr. Starnes, as Director General of the Security Service, was unable to obtain a Cabinet decision on how to resolve the dilemma of the apparent need of some undercover operatives to commit offences in order to maintain their credibility with violence-prone groups.[7] The policy issues associated with the use of undercover operatives are too important to both the security of Canada and the quality of its democracy to be left entirely to investigative agencies to resolve.

**62.** In designing a system to control a security intelligence agency in the use of undercover operatives, a distinction must be made between those who are developed or induced to provide information and those who volunteer information or from whom information is obtained without the expectation that they will become established sources of information about a particular subject of investigative interest.[8] In our view, the use of the former type of individual who is induced by the promise of money or some favour or by political ideology, to provide information to the state about his supposed political associates, or who may be a member of the security intelligence organization temporarily living an undercover existence as a member of a targetted organization, requires a higher form of authorization and tighter method of control than the use of sources on a voluntary or occasional basis. Hence in the system of controlling the general level of investigation which we proposed above, ministerial authorization would be required for any investigations involving "developed human sources" and members operating undercover.

**63.** We realize that the distinction between 'developed' and 'undeveloped' human sources will not always be easy to make. After all, the use of undercover operatives involves human relationships whose essential characteristics are not as self-evident as those of mechanical devices. Still, in the vast majority of situations we think it should be reasonably clear whether or not a person is being cultivated as a continuing long-term source of information about a particular organization. But here again, we should note that, if the members of the security organization have no understanding of or respect for the principle at stake in distinguishing between the different types of undercover operatives and in requiring a stricter method of controlling the most intrusive type, then the system of control will be frequently by-passed.

**64.** Evidence of growing concern about the risks inherent in the use of human sources in particular is afforded by the fact that the governments of both Great Britain and the United States have in recent years established administrative guidelines governing the use of informants by investigative agencies. In England, the Home Office has issued an administrative circular on the subject[9] and

---

[7] We deal with this matter in detail in a subsequent Report.

[8] For a description of the different types of informants used by the R.C.M.P. Security Service, see Part III, Chapter 9, section A.

[9] *Home Office Consolidated Circular to the Police on Crime and Kindred Matters.*

in the United States, Attorney General Levi established guidelines for the F.B.I.'s use of informants.[10] The latter are more pertinent to our concern in this chapter as they pertain to the F.B.I.'s domestic security investigations whereas the British directive pertains to criminal investigations. The introduction to the F.B.I. guidelines states that "while it is proper for the F.B.I. to use informants in appropriate investigations, it is imperative that special care be taken not only to minimize their use but also to ensure that individual rights are not infringed and that the government itself does not become a violator of the law". In using informants for authorized investigations the guidelines require the F.B.I. to consider a number of factors, the first of which is

> The risk that use of an informant in a particular investigation or the conduct of a particular informant may, contrary to instructions, violate individual rights, intrude upon privileged communications, unlawfully inhibit the free association of individuals or the expression of ideas, or compromise in any way the investigation or subsequent prosecution.[11]

**65.** The tendency of undercover operatives to inhibit political association and dissent is particularly great in security intelligence investigations where the groups which are subject to investigation are, by definition, political. Excessive planting of secret state operatives in political organizations could have, to use the language of American Constitutional law, "a chilling effect" on the exercise of freedom of speech and freedom of association in Canada.[12] These values, which are now recognized as fundamental human rights by the Canadian Bill of Rights and Bills of Rights adopted by several of the Provinces, may in the future be entrenched in the Canadian Constitution. It is consonant with a proper concern for the effect of the use of informants on fundamental political rights that we have proposed to restrict "full" investigations, including the use of developed human sources and members undercover, to situations where there is reason to believe a group is participating in espionage, sabotage, foreign interference, serious political violence or terrorism. Adoption of this proposal would mean that undercover operations could not be targetted against groups whose subversive activity went no further than the rhetorical and written espousal of revolutionary ideas.

**66.** Given the very serious impact which the misuse of undercover operatives can have on civil liberties and our principle that the more intrusive the technique of information collection the higher should be the authority permitting its use, it might be asked why we are not recommending that judicial authorization be required for the use of undercover operatives. We are recommending a system of judicial warrants following approval by a committee of senior officials and the Solicitor General for the use of electronic surveil-

---

[10] *Attorney General's Guidelines for F.B.I. Use of Informants in Domestic Security, Organized Crime and Other Criminal Investigations*, 1976, section 15.

[11] *Ibid.*, section A(1).

[12] Some court decisions in the United States have held that the use of undercover agents and informants in certain situations may violate the guarantees of free speech and association in the First Amendment of the U.S. Constitution; see, for example *U.S.* v. *White* 120 Cal. Rptr. (1975) 94, 533 5.2d 222 and *Local 309* v. *Gates*, (1948), 75 F.Supp. 620 (N.D. Ind.).

lance, surreptitious entry, mail opening, and access to personal information beyond biographical information on government files. Why not also require judicial warrants for the use of undercover operatives? We rejected a requirement of judicial warrants for the more intrusive type of operative for two reasons. First, there is an unavoidable lack of precision in identifying those individuals whose use requires the approval of higher authority and those whose use does not. As we have stated, obtaining information through undercover operatives involves human relationships whose defining characteristics are more complex than those of mechanical devices. Second, we think that requiring a judicial warrant for an investigative technique as subtle and complex as the use of undercover operatives is apt to involve the judiciary too closely in the investigative process. We note that Attorney General Levi advanced a similar argument in explaining to a congressional committee in the United States his decision not to require judicial warrants for the use of informants in domestic security investigations:

> Extending the warrant requirement in this way would be a major step towards an alteration in the basic nature of the criminal justice system in America... It would be a step toward the inquisitional system in which judges, and not members of the executive, actually control the investigation of crimes. This is the system used in some European countries and elsewhere, but our system of justice keeps the investigation and prosecution of crime separate from the adjudication of criminal charges. The separation is important to the neutrality of the judiciary, a neutrality which our system takes pains to protect... We must ask ourselves whether the control of human sources of information — which involves subtle, day-to-day judgments about credibility and personality — is something judges ought to be asked to undertake. It would place an enormous responsibility upon courts which either would be handled perfunctorily or, if handled with care, would place tremendous burden of work on federal judges.[13]

*The need for ministerial guidelines*

**67.** In addition to the system of prior approval for the use of undercover operatives which we have recommended in section B of this chapter, we think that a set of guidelines approved by the Solicitor General should be developed on important policy issues which arise in the use of undercover operatives. A section of the R.C.M.P. Security Service Operations Manual deals with a number of the subjects that should be covered in such guidelines, but the manual itself has not been subject to ministerial approval. Once they are approved the guidelines should be publicly disclosed, although they need not contain information about operational techniques, the disclosure of which would endanger the security of operations. They should express the principles which govern the use of human sources and members undercover by the security agency — principles which should be open to public scrutiny.

**68.** Throughout this Report we have referred to various forms in which policy direction is issued by the R.C.M.P. Words used by the R.C.M.P. to describe

[13] Quoted in John T. Elliff, *The Reform of F.B.I. Intelligence Operations*, Princeton, Princeton University Press, 1979, p. 126.

these different forms include "directives", "bulletins", "policy", "guidelines", and "manuals". Further, some of these words are, on different occasions, used in different senses. The consequence appears to be that there is no clear and consistent understanding by those who receive the policy direction as to their obligation to comply with it. This was exemplified to us in the testimony of a senior officer who told us that he regarded the then existing policy prohibiting telephone tapping as a "guideline" but that he also considered it to be a "policy" and "to some extent" a "binding rule". On the other hand, according to his testimony, even though he considered it as a "policy", there had to be room for "discretion and the exercise of judgment" in the application of the policy (Vol. 34, pp. 5506-9). Another illustration of the problem arises in Bulletin OM-82. We discussed the contents of that bulletin in Part III, Chapter 8. That bulletin was issued by the Commissioner in 1980 to become a part of the Operational Manual of the Force. It contained a statement that "The following general guidelines must therefore be adhered to in future". The Commissioner has advised us that, notwithstanding his use of the imperative word "must" in the bulletin, he did not intend it to be an "order", with the exception of the part that indicated that all members are expected to comply with provincial statutes and municipal bylaws in relation to traffic. He says that the remainder of the bulletin is "only a guideline". We are very concerned about the uncertainty that apparently surrounds the meaning and effect of the different words used by those promulgating policy direction. We think it probable that members in the field have the same difficulty we have encountered in knowing how "binding" a "policy" or a "guideline" or a "bulletin" is, and therefore in anticipating what the consequences may be if they do what the document says should not be done or fail to do what the document says shall be done. It is important that members receive more guidance than a simple assurance that their conduct, if reasonable, will not be judged adversely. Of equal importance to the members having a clear understanding of what the consequence of a breach of policy direction will be is that there be a systematic and critical scrutiny of the interpretation and practical application of the policy directions which are issued. Such a review and scrutiny must take place both within the police force and the security intelligence agency and also outside of them. So that such review and scrutiny can be made outside, the Minister responsible should be advised of all policy directions issued by the Commissioner of the R.C.M.P. or the Director General of the security intelligence agency — whether they are called "policy", "guidelines", "directives", "bulletins", or "manuals". In this Report we frequently recommend that the Minister responsible for the security intelligence agency should issue guidelines to the agency. We are conscious that the word "guidelines" may be used in several senses, including a mandatory sense and a discretionary sense. It is important that members of the agency know whether a guideline is mandatory or discretionary, that problems of interpretation in the field be drawn to the attention of the management of the agency, and that the interpretation and application of the guidelines be the subject of continuing scrutiny by the Minister, the Deputy Minister, the Director General, and the Advisory Committee on Security and Intelligence.

**69.** In the paragraphs that follow we discuss those matters relating to the use of undercover operatives which have raised legal or policy issues in the past and should be dealt with by administrative guidelines approved by the Solicitor General and in some cases also by legislative amendment.

*The use of deceit*

**70.** The recruitment and use of undercover sources necessarily involve deceitful activities. Recruiting a member of a foreign intelligence agency or a terrorist group to become a source of information for Canada's security intelligence agency entails inducing an individual to commit an act of betrayal and to deceive his present associates. Penetration of a group threatening security by a member or agent of the security intelligence agency can be accomplished only through falsifying the member's or agent's true identity and purpose. While we recognize the inevitability of deceit in the tradecraft of a security intelligence agency, we think there are limits beyond which deceitful activity must not be permitted to go. One limit, which we have already insisted upon, is that the source's activities must be lawful. Another is that the security intelligence agency must not deceive Ministers or senior government officials, nor should it falsely allege that a Minister has given an undertaking to protect or assist an informant. The ministerial guidelines on undercover operatives should clearly identify the forms of deceit which are unacceptable.

*Lawfulness of operative's activity*

**71.** Throughout this Report we have taken the position that there must be no departures from the rule of law in the policies and practices of a security intelligence agency. That principle should certainly be applied to the use of undercover operatives — whether the individual is an undercover member of the security agency or a person outside the organization acting as a source. We do not think there should be a double standard of acceptable conduct. Ensuring both the lawfulness and effectiveness of undercover operatives will, as we indicated in Part III, Chapter 9, require some legislative amendments. First, the need for false documentation to hide the true identity of the undercover operative (normally a member undercover) will require changes in federal and provincial laws similar to those proposed in relation to physical surveillance. In addition to provisions in laws relating to motor vehicle registration, driver's licences and hotel registration, provision should also be made where necessary for obtaining false documentation in laws governing S.I.N. cards, passports, birth certificates and education certificates. This would alleviate the need to manufacture and obtain documentation in a manner that in the past has resulted or may have resulted in violations of the Criminal Code: section 320 (obtaining by false pretences); sections 324 and 326 (forging and uttering forged documents); section 335 (offences in relation to register); and, section 362 (personation at an examination). Secondly, federal and provincial tax legislation should be amended to permit security intelligence agency sources not to declare as income payments received by them from the agency. We arrived at this position after considering and rejecting the feasibility of a system that would deduct tax payments from the payments to the source. (For

example, it would be next to impossible to determine accurately the rate at which such payments should be taxed.) We think this legislative amendment is needed to protect the identity of sources and to avoid a situation in which members of the security intelligence agency advise paid sources not to declare their payments as taxable income and thus conspire with their sources to break the provisions of the Income Tax Act. Further, the government should ascertain whether there are other legislative requirements governing employer and employee relations which may relate to payment of human sources, compliance with which would result in disclosing the identity of the source, and should seek whatever amendments may be necessary to overcome these difficulties.

**72.** A third area in which legislative reform is needed if sources are to be used effectively and lawfully for security intelligence (or criminal intelligence) purposes is section 383 of the Criminal Code which is concerned with secret commissions. As our analysis in Part III, Chapter 9, pointed out, judicial construction of this section necessitates an amendment to provide expressly that neither an agent nor an employee commits an offence in providing information about a principal or employer if this is done in the course of an authorized security intelligence investigation. In addition to this legislative change the guidelines governing the use of undercover operatives should recognize the need to balance the damage to the relationship of trust between employer and employee or principal and agent which use of a source may entail, against the potential value of the information for the protection of national security.

**73.** There is one further change in the law to which we have given careful consideration. That is whether there should be provision in law to allow security intelligence agency undercover operatives to perform acts which would otherwise be offences in order to establish or maintain their credibility with the groups they are attempting to penetrate. The R.C.M.P. Security Service raised this issue in relation to problems encountered in penetrating Quebec terrorist groups in the late 1960s and early 1970s. As we reported in Part III, Chapter 9, we have reviewed the extent to which the operational branches currently identify a need for undercover operatives to commit offences to maintain credibility. While the current operational policies of the Security Service prohibit instructing a source to commit an offence, they appear to leave the door open for a source to become involved in a criminal offence by stating that

> The D.D.G. [i.e. the Deputy Director General] has ruled that *any* degree of source involvement in *any* premeditated criminal offence will be decided by Headquarters on the events of each particular case. The support of the A/Gs or other appropriate authority, will have a definite bearing on such decisions.

**74.** We consider that the existing policy is unsatisfactory. Premeditated criminal offences by security intelligence undercover operatives must not be permitted under any circumstances. We considered two possible changes in the law which would provide greater leeway for security intelligence informants:

(1) A statutory defence for the commission of certain offences.

(2) A system of prior approval whereby in clearly defined circumstances and under appropriate controls an undercover operative of the security agency could be authorized to carry out a range of acts which would otherwise be offences.

We have concluded that there is not sufficient need to change the law in either of these ways. In taking this position we acknowledge that there will likely be situations in which sources or members of the security intelligence agency will have to forfeit their credibility with targetted groups and their usefulness as undercover operatives in order to avoid unlawful activity. This policy means that the security intelligence agency's informants will not be able to penetrate cells of movements in which the commission of an offence is the passport to admission, and will find it difficult, and in some cases may find it impossible, to play any role in violence-prone groups. But neither our extensive review of Security Service experience to date nor our speculation about future security threats, especially the threat of terrorism, has convinced us that the 'evil' to be thwarted is great enough to justify the 'evil' of secretly authorizing agents of the government to carry out a range of activities which would otherwise constitute criminal conduct, no matter how carefully and narrowly the criteria are drawn. The fact that the magnitude or urgency of future threats to security is unpredictable does not in our view justify stretching so ominously the leeway available under law to the agents of national security. Our conviction that the law should not be amended to expand the scope of lawful conduct by security informants is strengthened by recognition of legal mechanisms already available. The common law defences of necessity or duress might be of assistance to an operative in circumstances where the carrying out of an act which might otherwise be an offence appears to be the only means of avoiding serious bodily harm. Further, discretion in prosecuting and sentencing, as well as the prerogative power of mercy, may all be exercised in favour of a person whose criminal conduct can be shown to have been carried out for the purpose of protecting national security. The policy of the security intelligence agency should prohibit civil wrongs, as it would other unlawful conduct, on the part of undercover operatives. Nevertheless, there may be circumstances when such torts as we examined in Part III, Chapter 9 — inducement to breach of contract and invasion of privacy — may occur as the result of the activities of undercover operatives. If that should happen, and if individuals have suffered loss or damage as a result, the Crown should make *ex gratia* payments to them to compensate them.

**75.** The alternative to the position we have taken is to change the law so that under certain circumstances undercover operatives of the security intelligence agency could lawfully engage in conduct which would otherwise constitute criminal activity. This alternative could take the form of a provision in the Act governing the security intelligence agency whereby, under exceptional circumstances when the conduct is necessary to obtain information about a serious threat to security, a Committee of Ministers could, in advance, authorize the agency to permit certain of its members or sources to participate in conduct which would otherwise constitute a criminal offence. Such a provision could stipulate a limited range of permissible conduct that might well exclude either

bodily harm to persons or serious damage to property. The undercover operative of the security intelligence agency who engaged in such conduct would then not be committing an offence so long as the conduct was properly authorized and within the range of activity described in the Act. We have rejected this alternative and opted for the status quo because we think such an extension of investigative powers involves encroachment on civil liberty that would be a more serious evil than the damage to security resulting from the fact that the security intelligence agency lacks these powers. We realize that the position we have taken involves a certain risk that threats to security will go undetected. We also note that, in the United States, Guidelines governing F.B.I. investigations signed by Attorney General Civiletti on December 2, 1980[14] authorize "otherwise criminal" activity by F.B.I. informants under specified circumstances and subject to a prescribed approval process. These guidelines apply to both the domestic security and criminal investigation activities of the F.B.I. Because of the risk to security which our approach entails, we think that, if this approach were to be followed by the Government of Canada, its consequences should be carefully reviewed by the government and by the Special Parliamentary Committee on Security and Intelligence within 5 years. This review should attempt to adduce whatever evidence there is of damage to Canada's security resulting from the absence of any power on the part of security intelligence agency informants to commit "otherwise criminal" activity. This review should also examine as thoroughly as possible the experience of the United States and other western democracies that have adopted arrangements to authorize "otherwise criminal" activity by security informants.

*Reporting unlawful acts of undercover operatives*

**76.** Despite the policies and clear instructions of the security agency, an undercover operative might participate in criminal activity in the course of carrying out an assignment for the agency. Or the human source might participate in criminal activity unrelated to his work for the agency. Normally, in either case, the agency should report whatever knowledge it has of criminal activity to the law enforcement agency which has jurisdiction to investigate the activity in question. However, there may be situations in which the agency believes that the information an operative may obtain is of such importance to the protection of national security that information about the source's criminal activity should not immediately be turned over to law enforcement authorities. In situations of this kind where the requirements of law enforcement must be balanced against the needs of national security, the security agency must not be left on its own to determine which consideration should be given priority. When the agency thinks that the withholding of information about unlawful conduct of its sources is justified it should notify the Attorney General of Canada, who should be responsible for deciding whether or not the information

[14] *Attorney General's Guidelines on F.B.I. use of informants and confidential sources* (under the authority of the Attorney General as provided in 28 U.S.C. 509, 510, 533), Office of Attorney General, Washington, D.C., December 12, 1980.

should be turned over to the appropriate law enforcement authorities, according to arrangements we shall describe in Chapter 8 of this Part.

*Disruptive activities by undercover operatives*

**77.** As we reported in Part III, the Security Service sometimes has used undercover operatives as much for the purpose of disrupting or breaking up organizations as for the purpose of collecting information about them. In Chapter 6 of this part of our Report we shall set out our recommendations with regard to this type of disruptive activity: here we should note that the main recommendation we shall make — namely, that such activity should not be permitted outside of counter-espionage and counter-intelligence operations — should be incorporated in the guidelines governing the use of undercover operatives. Another kind of activity closely related to attempts by operatives to disrupt organizations consists of attempts to trap individuals in situations which will lead to their prosecution by provoking or instigating their participation in criminal activity. Because such attempts at entrapment or the activities of *agents provocateurs* are likely to occur more often in criminal investigations directed towards obtaining evidence to support a prosecution than in security intelligence investigations, we will deal with this problem in Part X, Chapter 5, where we consider legal reforms related to the criminal investigation responsibilities of the R.C.M.P. But aside from any changes which may be made in the Criminal Code to bar the use of evidence obtained in this way, the policy guidelines governing the use of undercover operatives should prohibit these individuals from instigating or encouraging unlawful conduct. Further, undercover operatives should be instructed to do what they can to influence groups who may be planning acts of violence to adopt milder methods of protest.

*Pretext interviews*

**78.** The security intelligence agency should not use the interviewing of a candidate for security clearance as an occasion for recruiting that person as a source. Such an abuse of the agency's security screening responsibilities is one which is most likely to occur in immigration and citizenship screening. It can have the unfortunate effect of making it appear to the applicant that he or she must agree to become an established source of information to the security agency as a condition for obtaining clearance. There may be circumstances in which a person interviewed in the course of security clearance proceedings appears to be an important source of information about a security threat which is currently under investigation. In those circumstances, if such a person is to be used as a source, the approach to him for recruitment purposes should not be made during the screening interview. The timing of the approach should be such that there is no possibility that the person will feel that he is being coerced into becoming a source. Preferably the approach should be made after the security screening decision has been made and communicated to him.

*Undercover operatives and the integrity of certain institutions*

**79.** There can be no doubt that the excessive or thoughtless use of security intelligence sources in certain contexts can have a very adverse effect on

institutions which are vitally important to our liberal democratic society. The current policy that requires ministerial approval for the use of paid sources who are to be used by the Security Service to gather intelligence solely on a university or college campus gives limited recognition to this point. Certainly the free flow of ideas and the freedom of inquiry so essential to the institutions of higher learning in a free society would be seriously threatened by the widespread planting of undercover operatives in colleges and universities. But colleges and universities are by no means unique in this respect. For example, the ability of journalists to obtain information essential to the functioning of an effective free press may be damaged if it is known or believed that journalists are widely used as security intelligence sources. Or, to take another sector of society, freedom of worship and religion may be adversely affected if priests or other religious functionaries are frequently employed to spy. The problem here is not only a source problem; it is a problem with undercover members who might seek to pose as teachers, journalists etc. The chilling effect is the same.

**80.** The threat posed to the integrity of institutions by the use of undercover intelligence agents has received considerable attention in the United States. The Senate Select Committee to Study Governmental Operations with respect to Intelligence Activities (the Church Committee) focussed attention on the risks associated with the use of academics, members of the media and of religious organizations as undercover informants. Draft legislation based on the Church Committee Report contains provisions prohibiting the use of membership in religious, media or educational organizations as a cover for an officer of an intelligence agency.[15] In Canada, only academic institutions have been specifically singled out in policy instruction as requiring particular sensitivity and control in relation to the use of sources. Mr. Dare indicated in his evidence before us that there is no policy with respect to other kinds of institutions beyond "the good common sense of very seasoned people..." (Vol. 318, p. 301693).

**81.** In our view the list of valuable institutions whose effective functioning may be adversely affected by the activities of undercover operatives extends far beyond academic institutions, the media and religious organizations. Labour unions and business corporations, cultural and ethnic organizations, for example, all of which play a valued role in our society, may also be adversely affected. Therefore, we think the guidelines governing the use of undercover operatives should reflect a general sensitivity to the damage which undercover operatives may do to all legitimate social, economic and political institutions. We think that sensitivity of this kind, exercised by security intelligence operatives in carrying out such investigations governed by the system of controls we have recommended, is preferable, as a basis for sound practice, to rules developed for specific areas such as those which now govern Security Service activity on university campuses. However, we acknowledge that the sensitivity required will not likely exist unless the recruitment and training of security intelligence officers are changed along the lines we shall recommend later.

---

[15] See *National Intelligence Reorganization and Reform Act of 1978 — s.2525* (The Huddleston Bill), s.132.

**82.** In calling for the security intelligence agency to exercise sensitivity to the integrity of valued institutions in using undercover operatives, we should, at the same time, recall a fundamental point we made in the earlier chapter on the scope of security intelligence surveillance — namely that no sector of society should be treated as immune to security intelligence investigations.

*Confidential relationships*

**83.** The use of human sources by a security intelligence agency may encroach upon confidential relationships in the private sector or between the citizen and government. For instance, the agency may wish to obtain information from lawyers or doctors about their clients or patients or from government officials who have access to personal data of a confidential nature.

**84.** As far as the private sector is concerned, as we reported in Part III, a security intelligence agency will come up against a number of legal difficulties when dealing with sources who are members of professional groups obliged to respect the confidentiality of certain kinds of information. The law of contract and tort may also create difficulties in the commercial sector. However, our assessment of the security agency's need for information did not convince us that the law needs to be amended (or clarified) to remove possible legal barriers to the security intelligence agency's use of sources in the private sector. There is one qualification we must make to this finding, pertaining to members of the medical profession. In preparing this Report we anticipated not being able to comment on such sources because we wished to wait until the report of the Ontario Commission of Inquiry into the Confidentiality of Health Information[16] (the Krever Commission) was available. That report has just recently become available and we have chosen to comment in one place on the several respects in which it touches upon matters of concern to us. Those comments are found in Annex I at the end of this Report.

**85.** The position we have taken with regard to the use of sources in the private sector who may be required by law not to provide certain kinds of information means that the security intelligence agency must have the assistance of a well-qualified legal adviser. The security agency must not violate legally protected confidential relationships in its use of sources. In determining whether or not legal difficulties exist, the security agency must not be guided by amateur and simplistic assessments of these difficulties. The law in this area is complex and dynamic, and the need for experienced and highly qualified legal advice is one of the reasons for our recommendation, in Part VI, for a Legal Adviser.

**86.** Turning now to the public sector, we think it is wrong for the security intelligence agency to use undercover sources in government departments to obtain confidential government information. The Security Service is now legally barred from obtaining access to certain kinds of biographical and personal information in federal government information banks which we think

---

[16] *Report of the Commission of Inquiry into the Confidentiality of Health Information*, Toronto, 1980.

it should have for authorized security investigations. In section H below, dealing with access to confidential information, we shall recommend certain changes in federal law to facilitate the access which we believe is required. Section 8(2) of the government's proposed Privacy Act (Schedule II of Bill C-43 which had its first reading on July 17, 1980) could permit access to confidential personal information:

> (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information disclosed;
>
> (l) for any purpose where, in the opinion of the head of the institution,
>
> (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.

It should be noted that in relation to subsection (l), the R.C.M.P. is designated, for purposes of the Act, as a "government institution". The government's proposed legislation on this subject would establish means of access for a security intelligence agency to personal information held by federal government departments and agencies. Our own proposals set out a more exacting system of control and review. This is the only way in which a security intelligence agency should gain access to confidential personal information in the possession of the federal government.

**87.** The policy which we recommend as appropriate for obtaining information from federal government departments and agencies should also apply to obtaining information from provincial and municipal governments. The security intelligence agency should not develop undercover sources within provincial or municipal governments as a means of obtaining access to information held by these governments. In Part III, Chapter 9, we reviewed provincial laws which govern access to information used in past operations by the Security Service. With the exception of hospital and health insurance records, on which we shall comment in Annex I, where we examine the relevant recommendations of the Krever Commission, we have concluded that there is no need to seek the co-operation of the provinces in obtaining amendments to laws protecting particular kinds of information. Nor do we think there is any need to seek exemptions from secrecy provisions of general application. In most cases, such as the civil servant's oath of secrecy, where government information is protected by general secrecy provisions, there is a convention that a Minister or head of department or agency has a discretionary power to disclose information. The proper course of conduct for a security intelligence agency which wishes access to such information is to request it from the Minister or official who is authorized to release the information.

**88.** We realize that a policy of confining the security agency's access to provincial or municipal government information to what can be obtained lawfully through authorized channels of communication precludes 'targetting' a provincial government which is suspected of supporting or participating in activity threatening the security of Canada. This would rule out, for instance, using a member of a provincial government as a source of information about

that government's suspected involvement in clandestine foreign interference in Canadian political life. As we pointed out in Part III, a municipal or provincial official who 'spies' on the government which employs him, may, among other things, violate section 111 of the Criminal Code which defines the offence of breach of trust by a public officer. But aside from legal prohibitions, we think it bad policy in a federal state for one level of government to spy on the other. While federal and provincial governments have had serious differences, including differences about Canada's constitutional future, these differences have not been about the fundamental importance of maintaining the democratic process of government, the protection of which is the ultimate purpose of national security arrangements. We think it would be unreasonably pessimistic to foresee a change in that situation sufficient to justify amending the laws of Canada to permit a national security intelligence agency to use undercover sources within provincial or municipal governments.

*The distinctiveness of security intelligence sources*

**89.** We have found that the effectiveness of a security intelligence agency may be adversely affected if in its treatment of long-term undercover sources it is too closely influenced by attitudes that policemen usually have to "informers". Policemen do not hold such persons in high regard. They tend to think of informers in the drug world, for example, in much the same way as they do criminals. Consequently a policeman finds it very difficult to understand that a long-term agent in place, such as a member of a political group who reports to the Security Service regularly on the activities of the group, is a different kind of person. He finds it hard to undertand that many such sources have originally volunteered to help the R.C.M.P. not because of a prospect of payment of money but because of their own concern that the activities of the group, or of some members of the group, are inimical to the interests of Canada. He finds it hard to understand that many such sources continue to lead their double life, sometimes at continuing risk of personal danger, and frequently at the expense of their own normal vocational development and personal life, not solely because of what money they are paid but because of a moral commitment to serve Canada. That motivation often *is* present. Yet it was reported to us that in 1980 a very senior officer in the R.C.M.P., all of whose experience had been on the criminal investigations side of the Force, when addressing a large group of members of the Security Service, spoke of some human sources in extremely derogatory terms. Nothing could have demonstrated more clearly to his audience that he and others like him, with criminal investigation backgrounds, were unlikely ever to be able to understand the handling of security intelligence sources, perhaps the most difficult aspect of investigative work, by a security service.

**WE RECOMMEND the establishment of administrative guidelines concerning the principles to be applied in the use of undercover operatives by the security intelligence agency. These guidelines should be approved by the Solicitor General, as the Minister responsible for the security intelligence agency and should be publicly disclosed. These guidelines should cover, *inter alia*, the following points:**

**(a) the forms of deceit which are unacceptable;**

(b) sources and undercover members must be instructed not to participate in unlawful activity. If an undercover operative finds himself in a situation where the commission of a crime is imminent, he must disassociate himself, even at the risk of ending his involvement in the operation. In situations where there is time to seek advice as to the legality of a certain act required of the undercover operative, such advice should be sought. If the act is considered to be unlawful, alternative courses of action should be considered. In many situations, this will allow the operative to continue in his role while remaining within the law;

(c) undercover operatives should not be used in situations where it is likely that the operative will be required to participate in unlawful conduct in order to establish or maintain his credibility;

(d) the agency should report unlawful conduct by undercover operatives, in accordance with the procedures which we propose in Chapter 8 of this Part;

(e) undercover operatives must not be used for the purpose of disrupting domestic groups unless there is reason to believe such a group is involved in espionage, sabotage or foreign interference;

(f) undercover operatives should be instructed not to act as *agent provocateurs* and, in situations where they become aware of plans for violent activity, to do what they can to persuade the members of a group to adopt milder methods of protest;

(g) interviews of persons for security screening purposes should not be used as occasions for recruiting such persons as sources;

(h) great care should be taken in authorizing the use of undercover operatives to balance the potential harm to which the deployment of such individuals within a social institution may do to that institution against the value of the information which may be obtained;

(i) the security intelligence agency should respect confidential professional relationships and other legal barriers to the use of sources in the private sector and should be directed by expert legal advice as to the extent of such legal barriers;

(j) employees or persons under contract to the federal, provincial or municipal governments must not be used as undercover sources in regard to matters involving their government. Confidential information held by governments must be obtained through legally authorized channels; and

(k) the making of *ex gratia* payments for loss or damage suffered as a result of civil wrongs committed by undercover operatives. (17)

WE RECOMMEND THAT to facilitate the obtaining of false identification documents in a lawful manner for undercover agents of the security intelligence agency, federal legislation be amended, and the co-operation of the provinces be sought in amending relevant provincial laws, in a manner similar to that recommended for the false identification needed in physical surveillance operations. (18)

WE RECOMMEND THAT income tax legislation be amended to permit the security intelligence agency sources not to declare as income payments

**received by them from the agency, and that other fiscal legislation requiring deduction and remittance by or on behalf of employees be amended to exclude such sources.**

(19)

**WE RECOMMEND THAT section 383 of the Criminal Code of Canada concerning Secret Commissions be amended to provide that a person providing information to the security intelligence agency in a duly authorized investigation does not commit the offence defined in that section.**

(20)

## E. ELECTRONIC SURVEILLANCE

**90.** The interception of oral communications by technical devices is an important means of collecting information about activities threatening the security of Canada. This method of collecting information takes two different forms: the recording of telephone conversations ('wire taps') and the planting of hidden microphones ('bugging'). We have reviewed the use of these techniques by the R.C.M.P. Security Service, especially since 1974 when the use of electronic surveillance became subject to the terms of section 16 of the Official Secrets Act. This review has left no doubt in our minds as to the necessity of using electronic surveillance for the protection of national security. There are groups and organizations in the espionage, foreign intelligence and terrorist fields that are very difficult to penetrate by human sources. In numerous situations it is reasonable to believe that such groups or organizations constitute such a serious threat to the security of Canada that advance warning is needed of their intentions and plans. Moreover, this advance warning is needed before evidence of a particular criminal activity is available. Electronic surveillance will often be the only effective means of obtaining the information which the state ought to have in these situations.

**91.** However, while we have no doubt as to the necessity for electronic surveillance as a technique of collecting information, we have found a number of inadequacies in the law and procedures which now govern the use of electronic surveillance by the R.C.M.P. Security Service. We identified some of these inadequacies in Part III in our discussion of practices not authorized or provided for by law. Here we shall bring together those legal considerations with other matters of policy as a basis for recommending changes in these laws and procedures.

*Applications for warrants*

**92.** Under existing procedures, proposals of field units to use electronic surveillance are reviewed at Security Service Headquarters. This review includes obtaining an opinion from a lawyer from the Department of Justice as to whether the proposed target of electronic surveillance falls within one of the categories of subversive activities listed in section 16(3) of the Official Secrets Act. If Headquarters approval is obtained, an application is prepared for a ministerial warrant. The Director General of the Security Service then presents the application to the Solicitor General, often with an aide-mémoire setting out further details with regard to the application. The Director General swears to

the truth of the information contained in the application. Normally no one else has been present when the Director General presents the application to the Solicitor General, although often the Deputy Solicitor General and the Commissioner have been present in the same room but have not participated in any way in the application. Typically requests for warrants have been put to the Solicitor General just after the weekly meetings with the Commissioner and other senior members of the R.C.M.P.

**93.** We are satisfied that the Security Service at Headquarters has made a conscientious effort to review the merits of proposals by field units that an application be made to the Solicitor General for a warrant under section 16. The following statistics were provided to the Commission by the section responsible for the administration of applications for such warrants, and cover the period from July 1, 1974 to August 1, 1978: 55 requests from the field for such warrants were rejected by various levels at Headquarters. Seven of those, which were rejected initially, received favourable consideration upon re-application by the field units and the provision of additional information. Also, it is evident that the several Solicitors General did not comply with all requests for warrants made by the Security Service. Eleven applications made to the Solicitors General from 1974 to 1978 inclusive were refused. In several of these instances a warrant was subsequently granted when additional information was provided.

**94.** There are, however, a number of improvements which we think should be made in the procedure followed in applying and granting warrants. To begin with, the 'application' — the document sworn by the Director General — has often been very brief in describing the activities of the targetted person or organization. Frequently much of the detailed information advanced in support of the application was set out in an aide-mémoire which was not formally part of the application. Mr. Dare testified that he did not consider that he was swearing to the truth of the information in the aide-mémoire. We do not think that this is an acceptable way of complying with the statutory requirement that the Minister be "satisfied by evidence on oath" of the necessity of granting the warrant. The truth of all of the evidence advanced in support of the request for the warrant should be sworn to under oath. If there are important matters of evidence which the Director General cannot in good conscience personally attest to, he should bring with him members of the security agency who can, or their sworn affidavits.

**95.** In considering the merits of a proposal to use electronic surveillance for national security purposes, the Solicitor General should have more advice than is now available from officials of his Department who are not members of the security agency. Under the system we have proposed for approving full investigations (in which electronic surveillance is one possible investigative technique) a senior official from the Solicitor General's Department (most likely the Assistant Deputy Solicitor General for police and security) would be included in the committee which decides whether to request ministerial authorization for a full investigation. This same official should also be involved in assessing the case for using electronic surveillance. In addition we think the Deputy Solicitor General should not be excluded from the process of appraising

applications for warrants. We note that in Great Britain every application by the Security Service for a warrant to intercept communications is submitted to the Permanent Under Secretary of State at the Home Office "who, if he is satisfied that the application meets the required criteria, submits it to the Secretary of State for approval and signature of a warrant".[17] We think it would be simpler to have the Deputy Solicitor General present when the Director General of the Security Service presents a proposal for electronic surveillance. However, whether the Deputy Solicitor General approves applications before they are submitted to the Solicitor General or is present when the Solicitor General is considering an application, the essential point is to make sure that the Minister has the advice of the most senior and experienced officials of his Department in making such a decision. It is especially important for a new Minister in his first days of office to have the assistance of a reasonably experienced Deputy, who is not a member of the intelligence agency, in assessing applications for electronic surveillance.

**96.** We turn now to a more far-reaching proposal for change in the existing law and procedure. We think that the use of electronic surveillance for national security purposes should be based on a clearer and more precise standard of necessity, similar to the standard established in section 178.13 of the Criminal Code for the use of electronic surveillance in the investigation of crimes. Further we believe that a judge, rather than a Minister, should make the final determination of whether a particular application satisfies the statutory conditions.

**97.** The conditions under which electronic surveillance may be authorized for national security purposes are now defined in section 16 of the Official Secrets Act as follows:

> (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.

[17] Cmnd. 7873, April 1980.

It should be noted that subsection (2) establishes three different tests for the issuance of warrants. The Solicitor General may issue a warrant 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.

However, apparently little attention is given to identifying which of the three tests has been satisfied by the evidence sworn by the Director General under oath. The practice has been for the warrant to blend together all three tests and simply recite 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. . .

Perhaps this would not matter so much if the "evidence on oath" directed the Solicitor General's attention to one of the three tests. However, the so-called 'applications' which are the "evidence on oath" have usually *not* indicated within which category the Director General has considered the circumstances to fall.

**98.** Section 16(2) of the Official Secrets Act should be compared with section 178.13(1) of the Criminal Code which requires a judge to be satisfied

(a) that it would be in the best interests of the administration of justice to do so (i.e. to give the authorization); and

(b) that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

While we acknowledge that part (a) of this test is not appropriate for national security intercepts, we think that it is just as important in the national security context as in the criminal investigation context that consideration be given to the factors set out in (b) in justifying the authorization of what otherwise would be an unlawful invasion of privacy by electronic means for those factors relate to necessity. We shall recommend that the statute governing electronic surveillance for national security purposes be amended to provide expressly the same criteria as those required to be satisfied under section 178.13(1)(b) of the Criminal Code and additional criteria that are pertinent to the collection of security intelligence. This should not be interpreted as requiring the security intelligence agency to exhaust other investigative measures before it can obtain a warrant. The section in the Code does not require that as a condition; it is only one of three alternative prerequisites. To require as a condition that other investigative measures have been exhausted would be unduly restrictive, for, as

in the case of criminal investigations, there undoubtedly will be circumstances in which no other investigative measures have even been attempted, and from the very circumstances of the case it would be impractical to carry out the investigation of the matter using other investigative procedures only; or the matter may be specially urgent.

**99.** In addition to incorporating the tests contained in section 178.13(1)(b), a clearer and more appropriate test should be adopted for assessing the national security purposes to be served by electronic surveillance. The confusing tripartite test now contained in section 16(2) of the Official Secrets Act should be replaced by language requiring that the person issuing the warrant be satisfied by evidence on oath that the use of an electronic surveillance technique is necessary for obtaining information about any one or more of the following activities:

> (a) activities directed to or in support of the commission of acts of espionage or sabotage (espionage and sabotage to be given the meaning of the offences defined in sections 46(2)(b) and 52 of the Criminal Code and section 3 of the Official Secrets Act);
>
> (b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;
>
> (c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country.

The warrant should indicate the type of activity of which the targetted individual or premises is suspected. In the previous chapter we have set out our reasons for preferring the wording set out in (a), (b) and (c) above to that which is now used in the definition of subversive activities in section 16(3) of the Official Secrets Act. Briefly it should be recalled that this language, among other things, makes it clear that electronic surveillance might be used to collect information about terrorist groups whose activities are directed against foreign countries and eliminates the dangerously broad and ambiguous phrase

> (c) activities directed toward accomplishing governmental change within Canada or elsewhere by force or violence or any criminal means.

Indeed, as we explained in the previous chapter we believe that intrusive investigative techniques such as electronic surveillance should not be used when there is no reason to believe that the activity of an individual or group goes beyond the expression of revolutionary subversive ideas.

**100.** With the adoption of clearer and more precise statutory tests for using electronic surveillance to obtain information about threats to national security, we think it would be appropriate for a judge rather than a Minister to issue warrants for national security intercepts. Earlier in this chapter, we presented our principal reason for requiring a judge rather than a Minister to make the authoritative determination of whether the facts of a particular case satisfy the statutory standard for the use of certain extraordinary investigative techniques. But here let us consider what might be the most formidable objections to our

recommendation to have a judge rather than a Minister issue warrants authorizing electronic surveillance.

**101.** First, it might be argued that the question of whether an individual or group constitutes a sufficient threat to national security to justify an electronic intrusion should be decided by Ministers who, unlike judges, are accountable to Parliament and ultimately to the electorate for national security policies. We agree with part of this argument. Ministers are responsible for the national security activities of government; in particular, the Solicitor General, as the Minister responsible for the security intelligence agency, is responsible for the investigative policies and practices of that agency. That is why we think the Solicitor General should approve proposals by the agency to use electronic surveillance (and other intrusive techniques). He should approve such proposals from a policy point of view. But he and the Cabinet must discharge their responsibility for national security policy within the law. When the law establishes a carefully defined standard for exercising an investigative power which would otherwise be a criminal offence, there is, in our view, no derogation of ministerial responsibility in denying Ministers the final authority to determine whether a particular case meets that standard. Our system of government is not based on the single principle of ministerial responsibility: it involves other important principles, one of which is the rule of law. In a system of responsible Cabinet government operating within the rule of law Ministers are responsible for the effective and proper execution of the powers lawfully available to government, but they do not have the final responsibility for determining what the law is. In our system of government this is normally the function of judges.

**102.** We should emphasize that we are not suggesting that the Minister should be indifferent as to whether a proposal to employ electronic surveillance meets the legal requirements. On the contrary, he and his advisers should thoroughly scrutinize proposals from a legal as well as a policy point of view before approving an application for a judicial warrant. But our review of the administration of section 16 of the Official Secrets Act has indicated to us that there is not sufficient assurance that in every case Ministers will carefully and judiciously apply their minds to all of the legal requirements for the use of this extraordinary power. We think that judges are more apt to have the appropriate experience and to be operating in an appropriate setting for making that kind of determination of the law. As we argued earlier, normally the courts determine the legality of government action only when it is challenged after the fact. However, because the effective use of this power should always be secret, no such *ex post facto* challenge is possible by persons who may be subject to an unlawful exercise of the power. Therefore, we think it necessary that a judicial determination of lawfulness be made before the power is exercised.

**103.** A second possible objection to our proposal is that it is too cumbersome and imposes too many procedural requirements on the conduct of national security investigations. Granted, the proposal would add one extra step to the decision-making procedure; we do not think this constitutes a serious handicap. Since the aim of most national security investigations is to collect information well in advance of an actual act of espionage, foreign interference or terrorism,

an extra few hours should not, in most circumstances, mean that it becomes too late to obtain important information. To provide for the exceptional occasion, when even such a slight delay would jeopardize an important national security investigation, there should be an emergency clause allowing the Minister to authorize an electronic intrusion without a judicial warrant for a maximum of 48 hours. The use of this power in emergency circumstances should be reviewed by the independent review body we are proposing (the Advisory Council on Security and Intelligence) and that body should report to the Parliamentary Committee on Security and Intelligence any situations in which it believed that the emergency use had not been justified.

**104.** To ensure the availability of reasonably experienced judges to hear applications for warrants, we propose that five judges from the Trial Division of the Federal Court of Canada be designated by the Chief Justice of the Federal Court to hear applications. If it were considered desirable to have judges available outside Ottawa for this purpose, there are members of provincial superior courts who, at the request of the Chief Justice of the Federal Court and with the approval of the Governor in Council pursuant to section 10(1) of the Federal Court Act, act as judges of the Federal Court. They are resident across Canada and some of them might be designated to review emergency applications. However, this may not be necessary, as the warrants issued under section 16 have, so far as we know, always been applied for and granted in Ottawa, with the exception of the occasional case when the Director General has had to go to the Minister when the latter was outside Ottawa. We think that the refusal of a judge to grant a warrant should be appealable to three judges of the Federal Court of Appeal. This would ensure the government some recourse in the event that a judge of first instance adopted what appeared to be a particularly idiosyncratic view of the law. To prevent 'judge shopping', an applicant should be required to disclose to the judge the details of any application made previously with respect to the same matter.

**105.** We believe that the choice of the best procedure should be based on an appreciation of Canada's security needs and the working of Canadian institutions of government. Nevertheless, it is relevant to ask those who believe that Canada's national security will not be adequately protected, if Federal Court judges rather than Ministers grant warrants for electronic intrusions, to examine the experience of the United States. There, although the United States Constitution assigns the President power over foreign affairs, since 1978 the use of electronic surveillance within the United States for foreign intelligence purposes has been governed by an Act of Congress which, whenever the communications of United States persons are involved, requires an order approved by a Federal Court judge based on an application approved by the Attorney General of the United States.[18] We are not aware of any submissions by the executive branch in the United States to the effect that the requirement

[18] *Electronic Surveillance Within the United States for Foreign Intelligence Purposes*, Public Law 95-511, 95th Congress, October 25, 1978.

of judicial warrants for national security intercepts has significantly weakened the investigative capacities of that country's intelligence agencies.

**106.** The procedure we propose might also be objected to on the ground that it does not go far enough to ensure the proper application of the law governing electronic surveillance for national security purposes. Hearings before a judge in our proposed system would be *ex parte* proceedings. As is now the case with applications for warrants under section 178.15 of the Criminal Code and under section 443 governing search warrants, no one would be present to argue against the application for the warrant. Submissions have been made to us that the proceedings should be made more adversarial by providing for the appointment of an officer to serve as 'a friend of the court'. This officer would appear before the judge and point out possible weaknesses or inadequacies in applications. While we think such a proposal has considerable merit and have considered it carefully, we have concluded that, on balance, it would not be advisable to adopt such a mechanism. The adversarial element afforded by such a procedure might be rather artificial and would make the process of approving applications unduly complex. Further, we think that an experienced judge is capable of giving adequate consideration to all relevant aspects of an application without the assistance of an adversarial procedure. Finally, the continuing and systematic review of the use of extraordinary powers by our proposed independent review body (the Advisory Council on Security and Intelligence) should provide an adequate means of ensuring that the system of control is working as was intended by Parliament.

*Renewals of warrants*

**107.** In Part III, Chapter 3, we pointed out that, in contrast to section 178.13(3) of the Criminal Code, section 16 of the Official Secrets Act makes no provision for the renewal of warrants. We also noted that, despite the absence of legal authorization for renewals, Solicitors General at the end of each year approved the renewal of large batches of warrants. This deficiency in the law governing electronic intrusions for national security purposes should be remedied. The law should not only require, as it now does, that the warrant specify the length of time for which it is in force, but it should also establish a maximum time period for warrants and require that an application for a renewal be treated as if it were a new application. We would suggest a maximum period of 180 days. While this would be approximately 60 days shorter than the average length for warrants in the last four years for which reported statistics are available, still it is three times the maximum period available under section 178.13 of the Criminal Code for electronic surveillance for criminal investigation purposes. The statute should require not only that an application for renewal should satisfy the same criteria as apply to an application for a warrant, but, in addition, that a report be made to the judge under oath as to the nature and value of the information obtained under the original warrant.

**108.** In the past there has not been a sufficiently thorough review of the 'product' of the interception of communications. Some interceptions have become virtually permanent. It is true that the vast majority of warrants which

are renewed and thus last for more than a short period of time are in respect of the communications of persons or establishments suspected of undertaking foreign intelligence activities, whether those persons are foreigners or Canadians. Even in these cases, in our view, there ought to have been a more critical review of the value derived from warrants for the interception of communications. From the point of view of the Solicitor General, in our opinion it is important that such a review take place in order that he can judge, with the kind of information which should be in his possession to enable him to reach a sound judgment, the extent to which interception is "necessary" for any of the purposes set forth in the statute.

*Conditions governing the execution of warrants*

**109.** Another inadequacy of the law governing the use of electronic surveillance for national security purposes which was thoroughly examined by us and reported on in Part III of this Report concerns the means which may be lawfully used to examine, to install, to maintain and to remove an electronic interception device. As we reported in Part III, Parliament, when it enacted the Privacy Act, did not explicitly provide for the surreptitious entries which are often essential for the effective use of certain kinds of listening devices and it is at least questionable whether section 26(2) of the Interpretation Act or section 25(1) of the Criminal Code provide a basis in law for the surreptitious entry of private premises or the removal of private property for the purpose of examining, installing, maintaining or removing devices the use of which might be authorized under section 16 of the Official Secrets Act. There is also doubt as to whether there is legal authority for using the electrical power available in the premises for the operation of a device. We think these doubts should be removed. Hidden listening devices cannot, in many instances, be used effectively without the surreptitious entry of premises or removal of private property. Also they cannot be used effectively without the use of electrical power belonging to or charged to the subject of investigation or another person. The statute should expressly provide that a warrant for the interception of private communications may permit the persons carrying out the interception to enter premises or remove property for the purpose of examining the premises or property prior to installing a device or for the purpose of installing, maintaining or removing a device. The statute should also provide for the use of the domestic electrical power supply. These powers should be available only on condition that their exercise shall not cause any significant damage to premises that remains unrepaired, nor involve the use of physical force or the threat of such force against any person. The statute should require the judge who issues the warrant to specify on the warrant the powers which may be used to execute it.

**110.** A further problem arises relating to the installation of electronic eavesdropping devices: the possible violation of provincial and municipal regulations governing such matters as electrical installations, fire protection and construction standards. As we suggested in our analysis of these problems in Part III, Chapter 3, we think that the co-operation of the provinces should be sought to make lawful what would otherwise be unlawful under the regulations in these areas.

**111.** A further condition which should attach to the execution of a warrant to intercept communications for security purposes is that in every case the persons carrying out the procedure should be accompanied by a peace officer. This recommendation is particularly important when our proposal to organize the security intelligence agency as a body separate from the R.C.M.P. is adopted. Under that proposal the members of the security intelligence agency would not be peace officers. In executing a warrant which may result in a breach of the peace by a person coming on the scene, we think it important that a policeman with peace officer powers be present. Moreover, as we shall explain more fully in subsequent chapters, the requirement that security intelligence officers obtain the assistance of a peace officer in executing warrants for extraordinary powers of investigation would add a valuable countervailing power in our security arrangements.

**112.** The statute should not require, as it does now, that a warrant "specify the person or persons who may make the interception or seizure". That is an unnecessarily exacting requirement and one which, as we indicated in Part III, is probably not being satisfied by existing procedures. We think it would be more satisfactory for the statute to provide that a warrant be issued to "the Director General of the security intelligence agency or to any persons who act upon his directions or with his authority". If the Director General proposes to use a person who is not a member of the agency or a peace officer, he should obtain the prior approval of the Minister to the use of such person.

*The scope of warrants for intercepting communications*

**113.** Considerable doubt and confusion have existed about the types of communication which may be intercepted and the range of investigatory activity which may be authorized pursuant to warrants issued under section 16 of the Official Secrets Act. Since 1976 warrants have been issued authorizing the interception and seizure of written communications outside the course of post. This was done after an opinion had been obtained from the Department of Justice in 1976 to the effect that written communications could be intercepted under section 16 other than letters in the course of post. Members of the Security Service have also on occasion, when on premises pursuant to a section 16 warrant, used the opportunity to rummage about and search the premises beyond what was necessary for the installation of a listening device. In Part III we reviewed all of these activities and the opinions on which they were based and reached the conclusion that section 16 of the Official Secrets Act likely did not authorize the interception or seizure of any kind of written communication including mail or the search of premises. We contended that if the Security Service needs the power to enter premises to examine written documents and remove them for copying, or to intercept mail or to search premises in circumstances for which a warrant cannot be obtained under the Criminal Code or under section 11 of the Official Secrets Act, then a case must be made to Parliament and legislation passed expressly authorizing such activities. These activities must not be carried out on the foundation of an interpretation of existing law that is not free from doubt.

**114.** Section 16 has also been used to authorize the acquisition from telephone and telegraph companies of copies of telegrams and telex communications. Also, section 7 of the Official Secrets Act provides for a special procedure under which authorization may be given by the Minister of Justice for the acquisition from any person who owns or controls "any telegraphic cable or wire, or apparatus for wireless telegraphy" of copies of telegrams and cables. This section provides that the Minister of Justice may grant a warrant in any case where it appears "that such a course is expedient in the public interest". Until early 1971, section 7 was relied on by the Security Service to gain access to telegrams, cables and telexes. "Telegraphic warrants" were issued under this section by Ministers of Justice from 1953 onward and served upon the telecommunications companies. The outstanding telegraphic warrants, like the telephonic warrants issued under section 11, were reviewed monthly by the Minister of Justice. It is not clear how long that procedure was followed. It is known that in 1971 the Solicitor General, Mr. Goyer, began to follow a new procedure. Telegraphic communications thenceforth were assimilated procedurally with telephonic communications. Instead of applying to the Minister of Justice for a warrant under section 7, the R.C.M.P. applied to the Solicitor General for his authorization, and, if it was granted, a senior officer of the R.C.M.P., in his capacity as a Justice of the Peace, would, pursuant to section 11, issue a warrant to search and seize directed to the telecommunications company. After July 1, 1974, when section 16 came into effect, that section was relied on for the warrants issued by the Solicitor General to acquire copies of telegrams and telexes. It is quite clear that the broad terms of section 7 which allow for warrants in any case where "such a course is expedient in the public interest" are inconsistent with the specific approach spelled out in section 16 and with the philosophy of this Report.

**115.** In subsequent sections of this chapter we shall recommend that legislation be enacted authorizing the security intelligence agency, under an appropriate system of controls, to search premises and photograph or make copies of documents and to open articles of mail in the course of post. These powers must be expressly provided for in legislation and, under our recommendation, would require warrants separate from a warrant for the interception or seizure of communications other than a message in the course of post. Legislation authorizing the issuance of the latter warrants for national security purposes should make it clear that communication means any oral or written communication other than a message in the course of post. There are written communications such as opened letters no longer in the course of post, and telex messages, the interception or seizure of which may be as important for national security purposes as is the interception of oral communications. But the statute governing these warrants should require, as does section 16(4) of the Official Secrets Act, that a warrant specify the type of communications to be intercepted or seized.

**116.** As recommended in the preceding paragraphs, there should be a single statutory provision like section 16 to be relied upon as authority for obtaining the contents of telephonic communications, non-telephonic conversations, and messages passed by mail, telegram, cable or telex whether acquired by

electronic means or by acquiring copies of the printed message. Therefore, the statute should contain a clear definition of "interception" so as to cover all these situations. We suggest that this definition read as follows:

> "interception" includes listening to, recording or acquiring any communication, any written communication other than a message in the course of post, and any telecommunication, and acquiring the substance, meaning or purport thereof.

*The communication of intercepted information*

**117.** A further deficiency in section 16 of the Official Secrets Act which we discussed in Part III is that there is no protection in law for a member of the Security Service who communicates information obtained through an authorized interception to other members of the Security Service, to other departments of the federal government or to provincial, municipal or foreign governments for security intelligence purposes. We think that protection should be afforded to members of the security intelligence agency who communicate information obtained from authorized interceptions, providing such communication is for the purposes of the security intelligence agency and is in accordance with reporting rules approved by the Minister.

*Reporting to Parliament*

**118.** Section 16(5) of the Official Secrets Act requires an annual report to Parliament on the use of warrants issued pursuant to section 16. The subsection reads as follows:

> (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.

A report formally satisfying the requirements of subsection (5) has been filed for the years 1974 to 1978 inclusive.[19] All of the statistical information reported for these five years in accordance with the requirements of (5)(a) and (5)(b) is contained in the table below.

---

[19] A report for 1979 was filed in 1980, after the preparation of this part of our Report.

*Statistics reported on use of warrants under section 16 of the Official Secrets Act, 1974-78*

| | 1974* | 1975 | 1976 | 1977 | 1978 |
|---|---|---|---|---|---|
| Number of warrants issued | 339 | 465 | 517 | 471 | 392 |
| Average length of time in force (in days) | 143 | 239.7 | 240.88 | 244.5 | 244.7 |

*6-month period only

**119.** The descriptive information required under subsection (c) and (d) has also been included in the annual reports to Parliament but in a very brief and standardized form. The "general description" of the methods of interception or seizure in the first two reports consisted of a reference to the fact that "wire tapping and eavesdropping by microphone" were used. The reports for 1976 added the information that the Solicitor General had issued a warrant authorizing the interception of postal communications but that "it could not be executed due to the prohibitive effect of section 43 of the Post Office Act". The reports for 1977 and 1978 indicated that in addition to wire tapping and eavesdropping by microphone warrants were issued for the "interception of written communication outside the course of Post". As for the "general assessment of the importance of warrants", each of the reports has contained virtually the same 'boiler-plate' language, as follows:

> (d) Warrants issued pursuant to section 16(2) O.S.A. have continued to prove of value in the detection and prevention of subversive activity both in the sphere of foreign intelligence activities directed towards gathering intelligence information relating to Canada and in the violent, terrorist or criminal activities directed towards accomplishing governmental change in Canada or elsewhere.
>
> Interceptions authorized by warrants issued pursuant to section 16(2) O.S.A. also proved indispensable investigative aids to supplement, verify or disprove information derived from other sources.

**120.** The bare minimum of information provided in these annual reports has not afforded Parliament an adequate basis for reviewing the operation of section 16 of the Official Secrets Act. The statistical information is apt to be misleading. For example, in giving the annual number of warrants issued, there was no disclosure that a number were merely renewals of warrants previously issued. Nor was there any disclosure that a number of the warrants issued in later years were renewals of warrants originally issued as early as 1974; that is, there was no way in which Parliament could realize that some warrants are, for all practical purposes, perpetual. The disclosure of "the average length of time for which warrants were in force" is misleading because, if the warrants that are virtually "perpetual" are treated separately, the "average length of time" for which other warrants were in force would be revealed as being significantly lower than the figure given. Above all, we regard as unhelpful the "boiler-plate" treatment of the requirement that the annual report provide "for the general assessment of the importance of warrants issued".

**121.** We recognize that there is a distinct problem of security in disclosing information about the use of electronic surveillance and other secretive investigative techniques which may be employed for national security purposes. That problem arises from the fact that hostile foreign intelligence agencies analyze for their own purposes every bit of information they can obtain about Canada's counter-intelligence activities. Information indicating a change in the deployment of our resources devoted to detecting foreign espionage and foreign intelligence activities may be of considerable use to such agencies. The report of the Birkett Committee in 1957 on the exercise of the power to intercept communications in Great Britain included statistics on interception for each year from 1937 to 1956. However, the Committee concluded that it would be wrong to disclose figures at regular or even irregular intervals on the grounds that

> It would greatly aid the operation of agencies hostile to the state if they were able to estimate even approximately the extent of the interceptions of communications for security purposes.[20]

Nevertheless, the very recent British White Paper on the Interception of Communications, in response to expressions of public concern about the extent of wiretapping and mail opening, has as "an exceptional measure" updated the Birkett Committee's figures. It reports the number of warrants issued by the Home Secretary for telephone wire taps and letter openings for each year since 1958. These warrants, it should be noted, may be issued in response to requests from the police and Customs and Excise officials, as well as from the Security Service.

**122.** We think that Parliament should have a sounder basis on which to review the exercise of the extraordinary power of investigation it has granted to the security intelligence agency. Annual statistics should be reported publicly on the number of warrants issued for each type of warrant which is available for national security investigation. (In addition to warrants for telephone wiretaps and eavesdropping by microphones, we shall be recommending warrants for concealed optional devices and cameras, or dial digit recorders, for surreptitious entries, for mail opening and for access to certain kinds of personal information held by government departments and agencies.) These statistics should clearly distinguish new warrants from warrants that are, in effect, renewals and indicate the frequency of renewals. With a statutory limit of six months on the period for which a warrant is available, we cannot see that any real purpose is served by requiring a disclosure of the average length of time of warrants. The statistical information which we propose should be annually reported may possibly be of assistance to hostile agencies. However, we think that this is a lesser evil than denying Parliament and the public an opportunity at least to monitor quantitative changes in the security agency's use of extraordinary investigative powers. The regular disclosure of accurate statistics is to be preferred to the irregular disclosure of information in response to public concern stirred up by public disclosures.

---

[20] Cmnd. 283, paragraph 152.

**123.** Turning to the qualitative assessment of the usefulness of the various warrants issued, we think that parliamentary review of this kind would be more effectively achieved through *in camera* meetings of a parliamentary committee than by 'boiler-plate' clauses in a public report. A full examination of the use of extraordinary powers cannot take place in public without risking great damage to the country's security. The Solicitor General should report annually to the Parliamentary Committee on Security and Intelligence his assessment of the usefulness of warrants issued in the past. In this forum, it should be possible for the Solicitor General to respond more thoroughly to questions arising from his report. Further, the independent review body (the Advisory Council on Security and Intelligence) which we shall propose, would have as one of its functions the monitoring of the entire system of special warrants for extraordinary investigative techniques. The Council's report to the Parliamentary Committee should assist members of the Committee in understanding how warrants are being used and how thoroughly the use of warrants is being reviewed by the security agency and the Solicitor General. The Parliamentary Committee should also be informed of difficulties encountered in interpreting or applying any of the statutory clauses governing the use of warrants. It should be possible to disclose much of the Committee's discussion of problems of this kind. Perhaps the wide discussion of the practice and procedure and substance of decisions made under section 16, found in this Report, and the extent to which the Government of Canada finds it possible to publish our discussion and lay it before Parliament, will provide an indication to the security intelligence agency and the responsible Minister in the future, as to what assessment and information might be laid before Parliament without imperilling the efficacy of the investigative technique or the work of the security intelligence agency generally.

*Intrusions of privacy by optical devices*

**124.** Long-distance viewing devices and miniature cameras are now available through which investigators can obtain photographs or video recordings of activities which occur or things which are located in places where there is an expectation of privacy. Future technological developments are likely to improve these devices and make them even more potent investigatory techniques. Although Parliament has not yet made it a criminal offence to oversee private communication or activity by these devices, still we believe that because they have as much potential for invading privacy as aural eavesdropping techniques, they too should be brought under an appropriate system of controls. We think that the use of hidden cameras by the security intelligence agency to film activities in places not open to the public should be lawful only under warrants issued by a judge under the same conditions as we recommended should apply to warrants for wiretapping and eavesdropping by microphone. This requirement, it should be noted, should not apply to cameras which are used in *public* places to assist in physical surveillance operations. We have not examined the use of intrusive viewing devices outside of the security context. However, this is a subject which may soon require the same legislative attention as the use of intrusive listening devices received a few years ago.

*Intrusions of privacy by "pen registers"*

**125.** An investigative device that is of occasional importance in intelligence collection is called a "pen register" by police forces. Its correct name is a "dial digit recorder". It is a small unit which is attached to a telephone company subscriber's line, usually by the telephone company. It may be used by the company to detect long distance toll frauds. It may be used by police forces and intelligence agencies to record the numbers dialled by a suspect, both local and long distance, in the expectation that this record will reveal who the suspect is dealing with. The device records the electronic impulses emitted by the subscriber's telephone when an outgoing call is made. Perforations on a tape attached to the device record the telephone number dialled, the date and time the call was made, and the duration of the call. Normally, the device does not record whether the receiving telephone was answered or the fact or substance of any conversation.

**126.** Legal opinions have been expressed by the Department of Justice and by one provincial attorney general that the use of pen registers does not constitute an "interception" of a "private communication" within the meaning of section 178.1 of the Criminal Code. We agree with that view. Likewise, we think that the use of pen registers need not be authorized by a Solicitor General's warrant under section 16 of the Official Secrets Act; nor need it be, for such use would not be an offence under section 178.11.

**127.** However, this leaves the policy question open. We think that a telephone subscriber has the same reasonable expectation of privacy in respect to the telephone calls he places as in respect to the communications he makes by telephone. The list of numbers called by a person may, just as much as a telephone conversation, reveal the most intimate details of a person's life. Knowledge that a list of numbers dialled from a telephone can be compiled by the police or a security intelligence agency without statutory authorization will inhibit the use of telephone facilities by some persons, such as journalists, in the legitimate exercise of their profession. If judicial support for the confidentiality of such information is needed, it may be found in *Glover* v. *Glover*.[21] Consequently, as in the case of the use of intrusive optical devices, even if there is no law making disclosure by the telephone company or the use of a pen register by anyone an offence, we think that the use of such devices by the security intelligence agency should be lawful only when there is a warrant issued by a judge and under the same conditions as we recommended should apply to warrants for wiretapping and eavesdropping by microphone.

**WE RECOMMEND THAT there continue to be a power to intercept communications for national security purposes but that the system of administering the power and the statute authorizing the exercise of the power be changed as follows:**

[21] (1980) DTC 6262 (Ont. C.A.). The case itself was concerned not with authorizing the use of a pen register but with whether the court in a child custody issue had the power to order the telephone company to disclose such information.

(1) All of the information on which an application for a warrant is based must be sworn by the Director General of the security intelligence agency or persons designated by him.

(2) Proposals for warrants should be thoroughly examined by a senior official of the Department of the Solicitor General and by the security intelligence agency's senior legal adviser, and the advice of the Deputy Minister should be available to the Solicitor General in considering the merits of proposals from both a policy and legal point of view.

(3) The legislation authorizing warrants should be amended so that, except in emergency situations, warrants are issued by designated judges of the Trial Division of the Federal Court of Canada on an application by the Director General of the security intelligence agency approved in writing by the Solicitor General of Canada.

(4) The legislation should authorize the judge to issue a warrant if he is satisfied by evidence on oath that the interception is necessary for obtaining information about any of the following activities:

(a) activities directed to or in support of the commission of acts of espionage or sabotage (espionage and sabotage to be given the meaning of the offences defined in sections 46(2)(b) and 52 of the Criminal Code and section 3 of the Official Secrets Act);

(b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;

(c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country;

and the warrant should indicate the type of activity of which the targetted individual or premises is suspected.

(5) The legislation should direct the judge to take the following factors into consideration in deciding whether the interception is necessary

(a) whether other investigative procedures not requiring a judicial warrant have been tried and have failed;

(b) whether other investigative procedures are unlikely to succeed;

(c) whether the urgency of the matter is such that it would be impractical to carry out the investigation of the matter using only other investigative procedures;

(d) whether, without the use of the procedure it is likely that intelligence of importance in regard to such activity will remain unavailable;

(e) whether the degree of intrusion into privacy of those affected by the procedure is justified by the value of the intelligence product sought.

(6) The legislation should provide that the Director General may appeal a refusal of a judge to issue a warrant to the Federal Court of Appeal.

(7) The legislation should provide that an applicant must disclose to the judge the details of any application made previously with respect to the same matter.

(8) The legislation should authorize the Chief Justice of the Federal Court of Canada to designate five members of the Trial Division of that court to be eligible to issue warrants under the legislation.

(9) The legislation should provide that in emergency circumstances where the time required to bring an application before a judge would likely result in the loss of information important for the protection of the security of Canada, the Solicitor General of Canada may issue a warrant which can be used for 48 hours subject to the same conditions which apply to judicial warrants. The issuance of emergency warrants must be reported to and reviewed by the Advisory Council on Security and Intelligence.

(10) The legislation should require that warrants specify the length of time for which they are issued and that no warrants should be issued for more than 180 days.

(11) Before deciding to make application to renew a warrant the Director General of the security intelligence agency and the Solicitor General should carefully assess the value of the intelligence product resulting from the earlier warrants. The legislation should stipulate that applications for renewals of warrants be treated on the same terms as applications for original warrants with the additional requirement that the judge to whom an application for renewal is made be provided with evidence under oath as to the intelligence product obtained pursuant to the earlier warrant(s).

(12) The legislation should authorize persons executing warrants to take such steps as are reasonably necessary to enter premises or to remove property for the purpose of examining the premises or property prior to installing a device or for the purpose of installing, maintaining or removing an interception device, providing that the judge issuing the warrant sets out in the warrant (a) the methods which may be used in executing it; (b) that there be no significant damage to the premises that remains unrepaired; and (c) that there be no physical force or the threat of such force against any person. The legislation should also provide for the use of the electrical power supply available in the premises.

(13) The Solicitor General should seek the co-operation of the provinces to make lawful what would otherwise be unlawful under provincial and municipal regulations governing such matters as electrical installations, fire protection and construction standards, in order to allow the security intelligence agency to install, operate, repair and remove electronic eavesdropping devices in a lawful manner.

(14) The legislation should provide for warrants to be issued to the Director General of the security intelligence agency or persons acting upon his direction or with his authority, but require that in every case the persons carrying out an entry of premises or removal of property in the course of executing a warrant be accompanied by a peace officer. If the Director General proposes to use a person who is not a member of the agency or a peace officer, he should obtain the prior approval of the Minister to the use of such person.

(15) The legislation should make it clear that warrants may be issued for the interception or seizure of written communications, other than a message in the course of post, as well as oral communications. Warrants for these interceptions must not be used for the examination or opening of mail or the search of premises. Section 7 of the Official Secrets Act should be

**repealed. (See Part IX, Chapter 2 for recommendation as to total repeal of the Official Secrets Act.)**

**(16) The legislation should exempt from section 178.2(1) of the Criminal Code the communication of any information obtained from an interception executed pursuant to the legislation by members of the security intelligence agency for purposes within the mandate of the security intelligence agency or for the purpose of enabling the Advisory Council on Security and Intelligence or the Parliament Committee on Security and Intelligence to review the operation of the legislation.**

**(17) The legislation should require that the Solicitor General annually prepare a report to be laid before Parliament indicating the number of warrants for interception which have been issued during the year, the number of these which constitute renewals, and the frequency of renewals and that the Solicitor General prepare a report for the parliamentary Committee on Security and Intelligence assessing the value of the intelligence products obtained from the warrants and problems encountered in executing warrants under the legislation.**

**(18) The use by the security intelligence agency of (a) hidden optical devices or cameras to view or film activities in places which are not open to the public and (b) dial digit recorders ("pen registers") should be permitted only under a system of warrants subject to the conditions of control and review as are recommended above for electronic surveillance.**

**(21)**

## F. SURREPTITIOUS ENTRY

**128.** We have reviewed the various situations in which the Security Service has conducted searches of private premises, vehicles or baggage to look for documents or other material that would provide information about the activity of an individual or an organization which threatens the security of Canada. We have also considered the extent to which such investigative practices are authorized in other jurisdictions and the extent to which future threats to Canada's security might require the authorization of these practices. On the basis of these deliberations, we have concluded that the law should be changed to authorize the security intelligence agency, in certain well-defined circumstances and under a thorough system of control and review, to search premises and property and to photograph and copy documents.

**129.** We have reached this conclusion reluctantly. As we stressed at the beginning of this part of our Report, in a liberal democratic state the intrusions of the state into the private life of its citizens should be minimized. Already numerous laws authorize agents of the state to enter and search private premises and remove materials without the consent of the occupant or the owner. No addition should be made to these laws unless it can be shown that it is necessary to do so in order to protect our society from a grave danger. It is because we think that the detection of threats to Canada's security requires a power of search not now available under law that we are prepared to recommend this particular change in the law.

**130.** One of the reasons for the need for special search powers consists of the activities of foreign intelligence agents. Foreign intelligence agents operate in Canada under diplomatic cover or sometimes as private individuals under false identity. Both kinds of agent are usually carefully trained to communicate in ways which will avoid detection. Situations arise in which evidence needed to corroborate suspicions that a person is acting as an undercover foreign intelligence agent takes the form of equipment used for secret communications such as code books, microdot or radio equipment or personal possessions which indicate the person's true identity. Past searches carried out by the Security Service have on occasion produced such corroborating evidence — or evidence discounting the suspicion, which may also be of importance in freeing a person from suspicion.

**131.** In the circumstances described above, a search warrant as provided for in section 443 of the Criminal Code would usually not be available or appropriate. That section sets out the conditions under which a justice may grant a search warrant as follows:

> 443. (1) A justice who is satisfied by information upon oath in Form 1, that there is reasonable ground to believe that there is in a building, receptacle or place
>
> (a) anything upon or in respect of which any offence against this Act has been or is suspected to have been committed,
>
> (b) anything that there is reasonable ground to believe will afford evidence with respect to the commission of an offence against this Act, or
>
> (c) anything that there is reasonable ground to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant,
>
> may at any time issue a warrant under his hand authorizing a person named therein or a peace officer to search the building, receptacle or place for any such thing, and to seize and carry it before the justice who issued the warrant or some other justice for the same territorial division to be dealt with by him according to law.

But there may be no reason to believe that there is anything in the premises of an individual suspected of developing a network of clandestine agents to work on behalf of a foreign power, which has been used or is intended to be used to commit a Criminal Code offence or will provide evidence of such an offence. Under current law, possession of espionage equipment, such as a code book or miniature camera, is not likely to point to any specific offence, nor do possessions indicative of a false identity. (In Part IX, Chapter 2, see the summary of our First Report recommendations with respect to possession of espionage equipment.) Further, even if a search warrant could be obtained for searching the premises of such a person, the procedure of obtaining and executing such a warrant will not provide for the secrecy which is necessary in counter-intelligence investigations. The opportunity of detecting the full range of a clandestine agent's network and of the capacity and intentions of his foreign handlers may be jeopardized if the search of his premises or possessions is disclosed.

**132.** The other provision of existing laws which might be thought to provide a sufficient basis for counter-espionage and counter-intelligence searches is section 11 of the Official Secrets Act which provides as follows:

> 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.

This section requires only suspicion, not belief, that an offence has been or is about to be committed and relates the search warrant directly to the espionage offences in the Official Secrets Act. However, in many investigations of persons suspected of developing a base for espionage or clandestine foreign interference there will be no grounds for suspecting a specific offence, e.g. that he has communicated information that might be, or is intended to be, directly or indirectly, useful to a foreign power. We think it is essential for the government to be informed of secret foreign intelligence activities at an early stage so that it can take action to expel diplomats or prevent undercover agents from penetrating security sensitive areas of government or industry. The security of Canada requires that much protection.

**133.** One further deficiency of section 11 of the Official Secrets Act should be noted. That section authorizes a justice of the peace to issue the warrant. Under section 17 of the R.C.M.P. Act, R.C.M.P. officers of the rank of Superintendent and above are *ex officio* justices of the peace having all the powers of two justices of the peace. We think it would be especially wrong for warrants authorizing such searches as section 11 provides for to be obtainable from R.C.M.P. officers if the security intelligence agency, contrary to our recommendation, remains within the R.C.M.P. But, even if our structural recommendation for a security agency separate from the R.C.M.P. is adopted, we think it inappropriate for special searches relating to espionage to be authorized by justices of the peace, whether or not they are R.C.M.P. officers. Searches of this kind should be authorized only by judges who are well-qualified to apply the terms of the statute to applications. Our recommendations below provide for such a system of authorization. On this basis, we see no point in retaining section 11 of the Official Secrets Act; the search and seizure powers in the Criminal Code should prove adequate for the enforcement by the police of the offences in the Official Secrets Act.

**134.** The other kind of activity which we think constitutes a sufficiently serious security threat to justify investigation through a special search power is political violence and terrorism constituting a grave threat to persons or property. Modern terrorist organizations frequently employ many of the methods used by foreign intelligence agencies. They develop clandestine communi-

cations links with foreign powers and endeavour to build up networks of support behind a safe cover. Situations have arisen in the past and are likely to arise in the future, in which it is reasonable to suspect that a person or group of persons are preparing for terrorist activity but in which there is no indication of a specific offence. For instance, when a foreign intelligence agency informs Canada's security agency of the presence in Canada of persons believed to have participated in serious terrorist acts in a foreign country, there may be no indication that such persons are planning any specific act in Canada. Because of the frightening means of destruction available to terrorists, and the tremendous damage to the democratic process which can result from terrorist threats to carry out acts of violence, we think the state should not have to wait until there is reason to believe that such threats are imminent before its security intelligence agency may be employed to search the premises or property of suspected terrorists. It is because we think that these politically motivated terrorist acts pose such a threat to the whole body politic that we are prepared to recommend legislation to make lawful certain kinds of searches by the security intelligence agency which have heretofore been unlawful. We are not however prepared to recommend a similar legislative change to render lawful 'intelligence probes' for other criminal investigation purposes.

**135.** Our support of this change in the law is conditional on the special power of search being subject to a system of control and review similar to that which we have recommended for electronic surveillance. That system, it will be recalled, would require that applications for such searches be first approved by the Solicitor General and then submitted to a Federal Court judge who would apply a statutory test as to the kind of activity about which information may be obtained and as to the necessity for using this particular investigative technique. Warrants would stipulate the time during which the warrant could be executed and the methods which could be used to obtain entry, and would require that the persons executing the warrant be accompanied by a peace officer. The use of the power would be subject to review by Parliament and by an independent review body in the same way that we have recommended for the review of electronic surveillance warrants.

**136.** The legislation authorizing searches for security intelligence investigations should make it clear that the premises which may be entered under warrants also include any vehicle, vessel or aircraft and that warrants may authorize examination of the contents of receptacles such as baggage and the temporary removal of written material for examination or for photocopying purposes.

**137.** It may be useful in assessing our recommendation to compare it with a similar proposal made by Australia's Royal Commission on Intelligence and Security. In the Report of that Commission, Mr. Justice Hope concluded that

> 164... ASIO (The Australian Security and Intelligence Organization) should have limited and controlled right of examination and search; the right should be exercizable only upon warrant granted by the Minister, and only where the Minister has been satisfied that there are reasonable grounds to believe that documents or records may be situated on the premises without which, or without intelligence concerning which, ASIO's

function of collecting security intelligence, in respect of an important matter under investigation, would be seriously prejudiced.

165. The right should not be exercizable in relation to domestic subversion unless the Minister is satisfied that the person or organization occupying or using the premises is already engaged in subversive activities.

166. These warrants, which should be exercizable at any time, should be limited to searching for documents and records, and should authorize their inspection, copying or removal. ASIO should be required to make a report to the Minister concerning the results of any such entry or search.[22]

This recommendation was closely followed by the Australian Parliament in enacting the Australian Security Intelligence Organization Act of 1979.[23] Section 25 of that Act provides as follows:

25. (1) Where, upon receipt by the Minister of a request by the Director General for the issue of a warrant under this section, the Minister is satisfied that there are reasonable grounds for believing that there are in any premises any records without access to which the collection of intelligence by the Organization in accordance with this Act in respect of a matter that is important in relation to security would be serious impaired, the Minister may, by warrant under his hand, authorize the Organization to do such of the following acts and things as the Minister considers appropriate in the circumstances but subject to any restrictions or conditions that are specified in the warrant, namely

(a) to enter the premises;

(b) to search the premises for the purpose of finding records relevant to that matter and, for that purpose, to open any safe, box, drawer, parcel, envelope or other container in which there is reasonable cause to believe that any such records may be found;

(c) to inspect or otherwise examine any records found in the premises and to make copies or transcripts of any record so found that appears to be relevant to the collection of intelligence by the Organization in accordance with this Act; and

(d) to remove any record so found for the purposes of its inspection or other examination, and the making of copies or transcripts, in accordance with the warrant and to retain a record so removed for such time as is reasonable for those purposes.

(2) The Minister shall not issue a warrant under this section on a ground that relates to domestic subversion unless he is satisfied that a person or organization occupying or using, or that has recently occupied or used, the premises specified in the warrant is engaged in activities constituting, or in preparation for, domestic subversion.

(3) A warrant under this section shall state whether entry under the warrant may be made at any time of the day or night or only during specified hours and may, if the Minister thinks fit, provide that entry may

---

[22] Australia, *Fourth Report of Royal Commission on Intelligence and Security*, Vol. I, 1977, p. 93.

[23] Australian Security Intelligence Organization Act, 1979, section 25.

be made, or that containers may be opened, without permission first sought or demand made and authorize measures that he is satisfied are necessary for that purpose.

(4) A warrant under this section shall specify the period for which it is to remain in force, being a period not exceeding 7 days, but may be revoked by the Minister at any time before the expiration of the period so specified.

(5) Subsection (4) shall not be construed as preventing the issue of any further warrant.

In one sense our proposal would go further than the Australian legislation, in that we would not confine such a search power to records but would extend it to espionage equipment and possessions indicating a false identity. But, in another sense, our proposal does not go as far as the Australian legislation in that we would limit the availability of this investigative technique to espionage, sabotage, foreign interference, serious political violence and terrorist activities, whereas in Australia the power could also be used in relation to domestic subversion. Under the definition section (section 5) of the ASIO Act of 1979, domestic subversion includes activities which are "likely ultimately" to involve the use of force or violence to overthrow the government and activities "directed to promoting violence or hatred between different groups of persons in the Australian community so as to endanger the peace, order and good government of the Commonwealth". Further it should be noted that our proposal would require that a different and, we believe, a more exacting test of necessity be applied in deciding whether to grant a warrant and that a judge rather than a Minister issue the warrant. Also, review by Parliament and an independent review body are not features of the Australian scheme.

**WE RECOMMEND THAT the security intelligence agency be authorized by legislation to enter premises, to open receptacles and to remove property for the purposes of examining or copying any document or material when it is necessary to do so in order to obtain information about activities directed towards, or in support of, espionage or sabotage, foreign interference or political violence and terrorism, providing that this investigatory power is subject to the same system of control and review as recommended above for electronic surveillance.**

(22)

**WE RECOMMEND THAT section 11 of the Official Secrets Act be repealed.**

(23)

## G. EXAMINING MAIL

**138.** In Part III we reviewed the Security Service's practice of obtaining information by examining the envelopes or covers of items being sent through the mail or by opening and examining the contents of such items, and concluded that these mail check operations violated provisions of the Post Office Act. (The Security Service's code name for these operations was "Cathedral".) However, at the end of that chapter we expressed the view that the law should be amended to permit the examination of mail to or from

persons if it is reasonable to believe they are engaged in activities dangerous to the security of Canada, providing such examinations are subject to an adequate system of control. Here we wish to elaborate on our reasons for taking that position and to put forward our recommendations for legislative changes.

**139.** Our assessment of the intelligence product of previous limited operations was that it has been of only marginal value. The following cases have been brought to our attention. One such operation was the investigation surrounding the Japanese Red Army terrorist, Omura. Two unauthorized Cathedral 'C' operations (mail openings) were performed during the Omura investigation, one authorized Cathedral 'B' operation (photographing or otherwise scrutinizing envelope but not opening it), and an authorized telephone interception. It is clear from the evidence that the telephone intercept provided evidence of a definite interest on the part of a Toronto resident in the affairs of the Japanese Red Army. However, this technique did not provide any specific indication of a link between the Toronto resident and Omura, until almost a year after the authorization for electronic interception was granted, when the terrorist arrived in Toronto.

**140.** The first Cathedral 'C' operation was undertaken to determine what other telephone lines were being used by the Toronto resident which might have to be tapped. This particular avenue proved inconclusive. Cathedral 'B' operations demonstrated the first concrete link between Omura (or "Joe", as he was known) and the Toronto resident when it was noted that on April 8, 1976, the Toronto resident received a registered letter from "Joe". The Toronto resident replied to "Joe" on April 13, 1976. This correspondence, as the second unauthorized Cathedral 'C' operation disclosed, consisted of two sets of applications to the University of Toronto, and established a clear link between the Toronto resident and Omura. It also established that Omura intended to visit Toronto. It is true that the telephone intercept had already indicated on April 12 that the wife of the Toronto resident had made inquiries at the University of Toronto concerning applications by foreign students in the Department of Political Economy, but, without the mail interception, that in itself would not have been sufficient to reveal the personal application of Omura.

**141.** Three R.C.M.P. members who testified before us concerning the case clearly indicated that they considered the use of Cathedral operations to have been vital to the resolution of this case. One of the witnesses indicated that without the results produced by the Cathedral operations, surveillance of the Toronto resident would not have been a priority item past April or May of 1976, and that, because of the scarce technical resources available to the Service, the telephone intercept would probably have been discontinued long before the expiry date of December 31, 1976, specified in the warrant. In other words, without opening the mail the Security Service would not have known that Omura intended to come to Canada, ostensibly to study, and the Service might have decided by the middle of 1976 to terminate its telephone tapping operation.

**142.** Another example of the use of mail opening by the Security Service will be published by us in edited form. Two Canadians who were members of an organization that the Security Service believed to be subversive travelled to a foreign country in the fall of 1970 and there was evidence that their expenses had been paid by a Canadian who was suspected of being a foreign intelligence agent. Earlier intelligence had suggested that this person had links with several violence-oriented Quebec-based revolutionary organizations. The Security Service had information that the country to which the Canadians were travelling was training guerrillas of other countries during 1969 and 1970. The Security Service was concerned that the violent guerrilla activity in that country and in another country might be planned for Canada. Consequently the Security Service began an intensive investigation in Canada of activities directed by what was "later established" to be the intelligence service of the foreign country. During the investigation, the Security Service opened the mail of the Canadian who paid the expenses of the two Canadians and other suspected agents. According to the Security Service, this helped to establish the identities of other persons whom the agent might be approaching to become agents of the foreign country in Canada, the mailing addresses of the foreign intelligence agency's handlers who were operating in several countries, and the links that existed with "several leading...Communists" both in Canada and abroad, who were supporting the activities of the foreign agents in Canada. The mail opening was complemented by surreptitious entries and electronic surveillance which produced evidence of cryptographic systems that were used by the Canadian-based foreign agents to communicate with the handlers in other countries; this enabled deciphering of the messages opened in the mail. The surreptitious entries also uncovered accommodation addresses being used by the foreign agency in several countries; helped in determining the channels and the amounts of money being used in financing the foreign agency's operators in Canada; helped to identify the structure and the executive of the revolutionary groups in Canada that were supporting the agents, and produced evidence that the Canadian who paid the travel expenses was being directed by the foreign agency and that he himself had recruited other agents in Canada. At the conclusion of the investigation, the premises of the three principal targets of the investigation were searched under warrants issued pursuant to section 11 of the Official Secrets Act, and the people were interviewed by the Security Service. No charges were laid, but one of the three returned to the foreign country to live there, and the Security Service believes that the activities of the foreign agency in Canada "subsided markedly after this event" (Vol. 315, p. 301406).

**143.** We also examined summaries, prepared by the Security Service, of 67 Cathedral 'C' operations, of which 55 had been authorized by Headquarters and 12 had not been so authorized. These 67 cases may be categorized as follows:

(a) 10 cases are considered by the Security Service to have produced an "important contribution to investigation". Of these 10 cases, the Security Service did not provide details as to the result in six cases; in four cases handwriting samples that were obtained proved to be useful; and in one the results were negative and were "important" only in the sense that they

contributed to the conclusion that the subject was not the agent of a foreign power.

(b) 17 cases are considered by the Security Service to be cases in which the opening of letters produced an "investigative lead", but no details of the "investigative lead" were given to us in 14 of the cases, and in a 15th case the information produced by the opening was a list of addresses of persons in contact with a suspected foreign agent. In the 16th case a known foreign intelligence officer had a close relationship with a federal government employee and once had been observed opening the employee's mail box; it was suspected that the employee was functioning as a "live letter box" (as a contact for mail to the intelligence officer), but the Cathedral "C" operation produced nothing of investigative value according to the summary provided (and contrary to the evaluation list provided). In the 17th case considered by the Security Service to have provided an "investigative lead", the envelope mailed by a known foreign intelligence officer was found to contain an application for a subscription to a small-town Canadian newspaper.

(c) In 12 cases the Security Service considers that "no intelligence of value" was obtained: in several, "semi-clandestine" contacts between the subject and a foreign military attaché had led to suspicions that Canadian military information might be passed; in another a Canadian had met clandestinely with an "agent of influence" of a foreign country; in most of the remainder of cases the subject was a known or suspected terrorist.

(d) In 16 cases, the Security Service reported that there was no evidence that mail was received.

(e) In 6 cases, Cathedral 'C', while authorized either at Headquarters or locally, was not carried out.

(f) The remaining 6 cases, while summarized, were not the subject of any evaluation by the Security Service as to whether the operation produced any intelligence of value. We do note that in one of these cases something of value appears to have been obtained: the names of the friends, relatives and contacts of a suspected foreign intelligence agent.

**144.** Two other cases are in the public domain. One is that of Mr. George Victor Spencer, the Vancouver postal employee who by 1960 had been recruited by a K.G.B. officer who was a member of the staff of the embassy of the U.S.S.R. According to the Security Service, Mr. Spencer admitted in his interrogation in 1965 that the tasks assigned to him included the use of his name and address as a "live letter box". Three test letters were sent to Mr. Spencer by the Soviet handler. As a signal, a small portion of a corner of the stamp had been removed and there was a small ink dot on the flap side of the envelope. His instructions were to deliver such letters unopened to his Soviet handler, who could thus examine them to determine whether they had been tampered with in the post. In addition, the Soviet handler made arrangements for meetings by sending an apparently innocuous message by mail, containing the date of the meeting. That message was to be responded to by an apparently innocuous letter of reply, which was to indicate whether the appointed date was

acceptable to Mr. Spencer.[24] During this investigation the Security Service says that it did not examine any of Mr. Spencer's mail, but speculates that the investigation might have been expedited if his mail had been opened. In any event, the case is useful as evidence of the use of the mail in Canada in an espionage operation.

**145.** So is the case of Mr. Bower E. Featherstone, a federal government employee who had access to classified material. Mr. Featherstone, when interviewed in 1966, denied having passed any classified material to the Soviet Union, but admitted that he had acted as a live letter box and had passed five letters from an unknown source to a Soviet handler and received payment for his services. Featherstone was charged and convicted under the Official Secrets Act because he had obtained and retained a naval chart which could have been "of assistance to a foreign power, to wit, the Soviet Union", (he had not delivered it). The use of Featherstone as a live letter box was disclosed in court by the Crown prosecutor.[25]

**145A.** In 1978 the officer in charge of counter-espionage reported that he had received information that a resident of Canada had requested instructions in what appeared to be an operation in an ethnic community in Canada. The R.C.M.P. Security Service suspected that instructions were given by letter, but because mail opening is illegal there was no way to find out.

**146.** Clearly, the case for recommending legislative authorization of mail examinations for national security purposes cannot be based solely on the value of the intelligence obtained from mail check operations in the past. These results of past operations do not settle the question of whether in the future, in order to obtain important information about threats to Canada's security, it may be necessary to examine mail, or the question of whether a law permitting the examination of mail of persons believed to be participating in acts directed towards or in support of espionage, secret foreign intelligence or terrorist activities will deter the use of Canada's postal system as a channel of communication for these activities. Our consideration of these two questions about the future brings us to recommend mail examinations for security purposes.

**147.** Agents of foreign intelligence services and members of terrorist groups are almost always very difficult to detect. They are usually individuals who are intelligent, dedicated to their cause, and well-trained in the art of avoiding detection by police or security officers. It is in their communication links that such persons are often the most vulnerable. We think it is unwise to guarantee them a free and convenient channel of communications within Canada by exempting all mail communications from lawful examination by security officers. Therefore, we believe it prudent that, in cases where there are reasonable grounds to believe that the mail is being used by persons for the

[24] Most of the foregoing was described in the *Report of the Commission of Inquiry into Complaints made by George Victor Spencer*, July 1966. The Commissioner was the Honourable Mr. Justice D.C. Wells.

[25] April 4, 1967. The prosecutor was Mr. P.T. Galligan, who disclosed this aspect of the case when speaking to the accused's sentence. The transcript does not reveal that the source of the information was Mr. Featherstone himself. See the *Ottawa Citizen*, April 5, 1967.

purpose of working secretly on behalf of a foreign power in Canada or of advancing the cause of a terrorist organization, the security intelligence agency should have access to any item in the course of mail as a means of furthering its investigation.

**148.** Against these considerations must be weighed the intrusion of privacy which will result. The mail is virtually the only means of communication left in our Canadian society into which the state cannot intrude without the individual's consent. A decision to weaken this one remaining citadel of private communication requires a very careful balancing of the respective weights which should be given to these competing concerns of national security and individual privacy. It is important to bear in mind that we are not dealing with absolutes. We doubt that the staunchest proponent of thoroughness in the protection of national security could demonstrate that Canada's security — as we have defined that concept — will be absolutely imperilled if Canada's security intelligence agency is denied the power of examining mail. But, by the same token, the privacy of postal communication would not be absolutely abolished for all citizens and residents of Canada by legislation which would permit a security intelligence agency, under judicial warrant, to examine the mail of persons who it reasonably believes are participating in espionage, foreign interference or terrorist activities.

**149.** This last point is important in that it refers to the conditions and controls which, in our view, must attach to an acceptable mail-opening system. Indeed our support for a legislative amendment authorizing mail examinations for national security purposes is conditional on such legislation prescribing conditions and controls similar to those which we have recommended for electronic surveillance and the search of private premises or property. An important objective of our review of the operation of section 16 of the Official Secrets Act was to assess the adequacy of that law as a means of regulating the interception of communications in national security investigations. Because of the many inadequacies we found in the provisions of that section and in its administration, we think it would be a mistake to extend that section to mail without redefining the conditions under which the power may be used and strengthening the system of controlling and reviewing its use along the lines we have recommended above.

**150.** One change in the provisions of section 16 which is particularly important in the context of mail opening is the definition of subversive activity in relation to which communication may be intercepted. Among other things, the definition which is now contained in section 16(3) makes it possible to intercept communications of persons whose subversive activity does not go beyond expressing ideas which call for the ultimate overthrow of our system of government or organizing a demonstration or protest strike to bring about a change in government policy. The definition of "subversive or hostile activities" found in section 15(2) of the Access to Information Bill recently tabled in the House of Commons (Bill C-43), is no improvement in this respect, as it still contains the dangerously ambiguous reference to

> (d) activities directed toward accomplishing government change within Canada or foreign states by the use of or the encouragement of the use of force, violence or any criminal means.

In our view the power to examine mail for the purpose of protecting national security should be used only if it is necessary to obtain information about an individual or group who, it is reasonable to believe, is engaging in activities directed towards or in support of espionage, sabotage, clandestine or deceptive actions to promote the interests of a foreign power in Canada, or acts of serious violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country.

**151.** Suggestions have been made that a power which constitutes so grave an encroachment on privacy as mail opening should be used only against foreigners, and not against Canadian citizens. Quite apart from obvious practical difficulties, we cannot accept this suggestion. It is not the nationality of individuals that determines whether their activities threaten security: it is the seriousness of the threat of these activities and the need to obtain advance information about them that constitutes the rationale for intercepting private communications. In any case, we look with disfavour on an approach to civil liberties in Canada which takes the position that the liberties which non-citizens in Canada may enjoy under Canadian law should be less than those enjoyed by citizens.

**152.** The system of granting warrants for the examination of mail and of reviewing the use of such warrants should be essentially the same as that which we have recommended for electronic surveillance and the search of private premises or property. Warrants should be issued to the Director General by a Judge of the Federal Court on the basis of an application approved by the Solicitor General and with evidence given under oath as to the necessity of using this particular investigative technique. The statute should direct the judge to consider the same matters in determining whether there is necessity as when hearing applications for warrants to intercept communications for purposes of criminal investigation under section 178.13(1)(b) of the Criminal Code. The use of warrants and the operation of the legislation should be subject to review by Parliament and the Advisory Council on Security and Intelligence on the same basis as recommended for electronic surveillance and searches of premises or property.

**153.** The legislation providing for the examination of mail by the security intelligence agency should require that a warrant be obtained for the examination of all classes and types of mail and for obtaining information from the envelopes or exterior covers of items in the course of post as well as from the contents of mail. The legislation should expressly state that its provisions for the issuing of warrants shall prevail over section 43 of the Post Office Act, and the latter section should be amended to make this possible.

**154.** Warrants should specify the ways in which articles are to be examined. It may be sufficient to obtain information from mail covers and not necessary to read the contents. There should be authorization for copying the covers or contents of mail, and for temporarily removing the article from Canada Post premises. We think it would be impracticable to adopt the suggestion made in one submission to the Commission that warrants specify the letters to be opened. It is impossible to predict the specific letters or parcels which may

contain relevant information or material. Warrants should be issued for the interception of mail addressed to, or sent by or from, a specified person or address. The latter possibility is necessary to provide for a situation in which it is suspected that a false name is being used. Warrants should also specify the length of time during which a warrant may be used within the same maximum time period and subject to the same renewal conditions as we have recommended for electronic surveillance and searches. We note that section 27(4) of Australia's ASIO Act imposes a 90-day time limit on warrants for postal inspections as compared with a six-month limit on electronic surveillance warrants. However, we cannot see why there should be a difference in the maximum periods for which the two kinds of warrants are available. In both cases, six months should be treated as a maximum and every effort should be made to confine the length of time for which a warrant is requested and granted to the period when it is reasonable to expect significant communications to occur. Because breaches of the peace do not occur in executing a warrant to examine an article in the course of post, it would make no sense to require that a peace officer be present when these warrants are being carried out. However, the legislation should require that the Post Office Department be informed whenever a warrant is issued and when warrants expire. Further the legislation should require the co-operation of postal officials with members of the security intelligence agency in carrying out the procedures specified in a warrant.

**155.** In judging whether articles of mail should be inspected for national security purposes and if so, under what conditions and controls this should be done, Canadians will no doubt wish to base their decisions on an assessment of Canada's security needs and on the ideals of civil liberty which derive from Canadian traditions and aspirations. Still, in arriving at a decision and in assessing the recommendations of this Commission on this subject, it may be useful to look at the laws and policies of countries whose system of government and democratic principles are close to our own. In the United States, although the Rockefeller Commission and the Church Committee disclosed widespread improper surveillance of the mails by intelligence agencies, U.S. mail is not made immune from lawful inspection for national security purposes. The President's Executive Order of January 21, 1978[26] attempted to control national security mail checks by providing that:

> 2-205. Mail Surveillance. No agency within the Intelligence Community shall open mail or examine envelopes in United States postal channels, except in accordance with applicable statutes and regulations. No agency within the Intelligence Community shall open mail of a United States person abroad except as permitted by procedures established pursuant to section 2-201.

Generally the control system is stricter where there is no suspicion of any foreign involvement. First class mail which originates in the United States cannot be opened without a showing of "probable cause" (i.e., a belief that evidence of a crime will be discovered) unless consent has been secured or an

[26] Executive Order 12036; January 21, 1978.

emergency exists. Letters opened for foreign intelligence purposes may be an exception to this rule. Mail cover checks are permitted under Postal Service regulations which require a written request from a law enforcement agency specifying "reasonable grounds" which demonstrate that the mail cover is necessary to

(a) protect the national security,

(b) locate a fugitive, or

(c) obtain information regarding the commission or attempted commission of a crime.[27]

The "reasonable grounds" requirement is a standard which appears to be less demanding than the "probable cause" requirement of the Fourth Amendment of the U.S. Constitution. In late 1978 a Federal Court Judge declared this national security ground to be unconstitutionally vague. In August 1979, new regulations were adopted by the Postal Service defining the phrase "to protect the national security" to mean:

> to protect the United States from any of the following actual or potential threats to its security by a foreign power or its agents:
>
> (i) an attack or other grave hostile act;
>
> (ii) sabotage, or international terrorism; or,
>
> (iii) clandestine intelligence activities.[28]

In Great Britain authorization to examine mail for criminal investigation, customs or security purposes is obtained through the same process of ministerial warrants as applies to telephone interceptions. The recent White Paper on this subject discloses that over the past 20 years the highest number of warrants for mail opening issued by the Home Secretary in any one year has been 139 and the lowest, 44.[29] However, these figures do not indicate how many of these warrants were issued for national security investigations. Finally, in Australia, following the recommendations of the Royal Commission on Security and Intelligence, provision for examining mail has been included in the Australian Security Intelligence Organization Act.[30] Warrants for examining mail are issued on terms and conditions similar to those set out in section 25 (reproduced above) with respect to searches.

> **WE RECOMMEND THAT, notwithstanding the present provisions of the Post Office Act, the security intelligence agency be authorized by legislation to open and examine or copy the cover or contents of articles in the course of post when it is necessary to do so in order to obtain information about activities directed towards or in support of espionage or sabotage, foreign interference or serious political violence and terrorism, providing that this investigatory power is subject to the same system of control and review as recommended above for electronic surveillance, except that**

---

[27] 39 C.F.R. 233.2.

[28] *Ibid.*

[29] Cmnd. 7873, April 1980, Annex, Table I.

[30] Australian Security Intelligence Organization Act, 1979, section 27.

**instead of requiring that a peace officer accompany persons executing warrants issued for this purpose, the legislation should require that the Post Office Department be notified when such warrants are issued and expire and that Post Office officials co-operate with members of the security intelligence organization in carrying out the procedure specified in the warrant.**

(24)

## H. ACCESS TO CONFIDENTIAL PERSONAL INFORMATION HELD BY GOVERNMENT

**156.** An important potential source of information for a security intelligence agency is personal information contained in the files and records — the so-called 'data banks' — of departments and agencies of the federal government. We say 'potential' source because under existing law the release of virtually all personal information held in federal government data banks to the R.C.M.P. is prohibited if the release is for security intelligence purposes. In the past, as we reported in Chapter 6 of Part III, the R.C.M.P. Security Service obtained confidential personal information from federal government departments notwithstanding that such practices were in some instances not authorized or provided for by law; however, in the past two or three years the legal barriers to access have been strictly observed.

**157.** At the conclusion of Part III, Chapter 6, we stated our view that the laws which protect the confidentiality of personal information held by the federal government should provide some means of access by the security intelligence agency to protected information, provided such access is subject to an appropriate system of control and review. Here we shall set out our reasons for recommending this change in the law and our recommendations as to the kind of legislative change which is needed.

**158.** Again, in considering this subject we must weigh our concern for the individual's privacy against the requirements for effectively protecting national security. Today, the enormous range of government programmes and regulation means that there are myriad circumstances in which the citizen is required to give personal information to the government in order to comply with statutory obligations or enjoy statutory benefits. Our concern about how this ever-growing volume of information which the government holds about each one of us is used, and how access to it is controlled, is not only a concern for individual privacy; part of our concern is with maintaining a relationship of trust between the citizen and government.

**159.** But it should also be recognized that there are important investigatory needs relating to the protection of national security which are most effectively met by affording the security intelligence agency access to certain kinds of government information. We think these needs should be served, and can be served, in a manner which will both prevent excessive disclosure of personal information and entitle the government to retain the trust of the citizen in its respect for the confidentiality of personal information.

**160.** The most important investigatory use of personal information in government data banks is in assisting the security agency in its efforts to identify and locate individuals. These efforts are particularly important when the subject of investigation is suspected of operating under a false cover, or when the agency is trying to discover the identity of a person reported to be in contact with a hostile foreign intelligence agency or to be associated with a terrorist organization. Information in government files is obtainable directly and expeditiously, and can often save considerable time and expense in ascertaining and corroborating identity. Information in the S.I.N. data bank, because of its universality, is one of the most useful sources of government information for this purpose.

**161.** Our review of cases in which the Security Service has used information in government data banks and cases in which it has requested to use such information disclosed several other important uses of this kind of information.

**162.** Occasionally, such requests have been made as the result of inquiries by foreign intelligence agencies. We think these requests of foreign intelligence agencies should be screened much more carefully than they have been in the past. In Chapter 7 of this part of our Report we make recommendations for strengthening the system of controlling liaison with foreign agencies and for ensuring that the security intelligence agency provides information to foreign agencies only on subjects that are within the Canadian agency's own statutory mandate. But within these limitations and controls, we think it essential that Canada's security intelligence agency be able to respond effectively to requests received from foreign intelligence agencies. The protection of Canada's security frequently requires that our own security agency obtain information from foreign agencies, including information held by departments of foreign governments about the identity of persons travelling with foreign passports in Canada. Our security agency's access to this foreign information is put in jeopardy if it cannot reciprocate by supplying information from its own government's files.

*Access provided for in proposed Privacy Act*

**163.** A legislative proposal which is currently before Parliament would remove the largest single legal barrier to a security intelligence agency's access to government information. This is the proposed Privacy Act which, along with the government's Bill on Access to Information, had its first reading in the House of Commons on July 17, 1980. This legislation could give the security intelligence agency a controlled means of access to all personal information held by government institutions except for information which is protected by other Acts of Parliament. It would accomplish this by repealing and replacing Part IV of the Canadian Human Rights Act. Section 52(2) of that Act provides as follows:

> (2) Every individual is entitled to be consulted and must consent before personal information concerning that individual that was provided by that individual to a government institution for a particular purpose is used or made available for use for any non-derivative use for an administrative purpose unless the use of that information for that non-derivative use is authorized by or pursuant to law.

When this "non-derivative use" section of Part IV became law in 1976, there was some doubt as to whether Security Service requests for information (or, for that matter, Criminal Investigation Branch requests) constituted a prohibited administrative use. However, by 1978, section 52(2) was being interpreted strictly by all departments and agencies with the result that the R.C.M.P. Security Service was now denied access to virtually all personal information possessed by other federal government institutions.

**164.** Section 7 of the Bill now before Parliament, which it is proposed should replace Part IV of the Canadian Human Rights Act, provides that personal information under the control of a government institution shall, subject to certain exceptions, be used only for the purpose for which it was obtained. Section 8(2) lists the exceptions, all of which are "subject to any other Act of Parliament". The exception which is most relevant for our purposes is 8(2) which would permit a government institution to disclose personal information

> (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

Assuming that the security intelligence agency would be an investigative body specified in the regulations, it would by virtue of this clause have access to personal information in all government data banks except those to which access is barred by other Acts of Parliament. One of the important sources of security intelligence to which this legislation would restore access is information which the Department of External Affairs' Passport Office has obtained from passport applicants. However, there is some doubt as to whether the security intelligence agency under the proposed legislation would have access to S.I.N. card information. As we said in Part III, Chapter 5, it may not be open to the Minister of Employment and Immigration to release S.I.N. card information for security intelligence purposes.[31] Nor would the agency have access to income tax,[32] family allowance,[33] old age security[34] or Canada Pension Plan information[35] or census information obtained by Statistics Canada,[36] all of

[31] Section 114 of the Unemployment Insurance Act (S.C. 1970-71 Chapter 48 as amended by S.C. 1976-77, Chapter 54, Section 60.1) provides as follows:

> 114. Information, written or oral, obtained by the Commission or the Department of Employment and Immigration from any person under this Act or any regulation thereunder shall be made available only to the employees of the Commission or the said Department in the course of their employment and such other persons as the Minister deems advisable, and neither the Commission, the said Department, nor any of their employees is compellable to answer any question concerning such information, or to produce any records or other documents containing such information as evidence in any proceedings not directly concerned with the enforcement or interpretation of this Act or the regulations.

[32] Income Tax Act (R.S.C. 1970, ch.148), s.241(1).

[33] Family Allowances Act, 1973 (S.C. 1973-74, ch.44), s.17.

[34] Old Age Security Act (R.S.C. 1970, ch.O-6), s.19.

[35] Canada Pension Plan (R.S.C. 1970, ch.C-5), s.107.

[36] The Statistics Act, S.C. 1970-71, ch.15, s.16.

which are protected by Acts of Parliament which bar disclosure of information, even with the permission of the Minister, for any purpose unrelated to the programme or purpose for which the information was obtained.

**165.** The proposed legislation would go some way towards improving the current situation. It would give the security intelligence agency access to some of the government information it must have if it is to discharge its functions effectively. Also, it would provide a system of controlling and reviewing this access which would be a distinct improvement on the haphazard and often underhand procedures that prevailed in the past. Requests for personal information would have to be made in writing specifying the purpose for which the information was needed. Requests would be made directly to the Minister or head of the institution which holds the information. Section 8(3) requires that the Minister or head of the institution must retain a copy of the request, and, if requested by the Privacy Commissioner, provide the Privacy Commissioner with a copy of the request. The Privacy Commissioner may review, either on her own initiative or in response to an allegation by a complainant, whether personal information has been properly disclosed. While these provisions of the proposed Privacy Act represent, generally, a move in the right direction, we think they fall short of a satisfactory comprehensive solution to the issue of providing access for national security purposes to personal information held by the federal government. In certain respects, the legislation goes too far in opening up access to a security intelligence agency and in other respects it does not go far enough.

*The scope of access*

**166.** First, let us deal with what we consider to be an inadequacy in the access provided for in the proposed Privacy Act — its limitation to data banks not protected by other Acts of Parliament. We think there are circumstances in which tax information will be an extremely valuable means of identifying or detecting persons who are acting covertly on behalf of a foreign power or who are furthering the objectives of terrorist groups. For these situations the law should provide for the security intelligence agency to have access to income tax information under an appropriate system of control and review. However, while information from Family Allowance, Old Age Security and Canada Pension Plan records is not as likely to be needed for security intelligence investigations, we cannot see why the law should not provide for the same limited access to these data banks. We note that the Church Committee in the United States — which is the only other government Commission or committee in the English-speaking democracies to report on this subject — came to a similar conclusion. While it called for tight controls on the intelligence agencies' access to tax records as well as medical or social history records, its recommendations on this subject would give access to such information

> (1) In the course of a criminal investigation if necessary to the investigation;
>
> (2) If the American is the target of a full preventive intelligence investigation and the Attorney General or his designee makes a written finding that

(i) he has considered and rejected less intrusive techniques; and (ii) he believes that the covert technique requested by the Bureau is necessary to obtain information necessary to the investigation.[37]

**167.** One category of federal government information which it would be reasonable to exempt from the scope of legislation giving access to otherwise protected bodies of information is the census information compiled by Statistics Canada. While such information may not be more personal than that found in some other federal data banks, the tradition in this country has been very strongly in favour of complete confidentiality of census returns. The unqualified guarantee of confidentiality helps to overcome the reluctance of Canadians to respond to inquiries about personal matters for purposes which may be suspect, or at least not clearly understood, by many.

*Control and review of access*

**168.** Turning now to the system of control and review provided for in the proposed Privacy Act, we think there are a number of ways in which that system should be strengthened. The legislation does not provide a clear enough test of necessity for access to personal information for security intelligence purposes. It leaves the prior approval of all access, including access to details of a person's life far beyond what is needed for purposes of identification, to Ministers, and it provides no role in approving requests for information to the Minister responsible for the security intelligence agency.

**169.** In our view a satisfactory system for controlling access by a security intelligence agency to personal information in the hands of government departments must recognize a distinction between two kinds of information requiring two levels of protection. There are a number of items of what we will refer to as 'biographical information' which are extremely useful in identifying and locating individuals and which are relatively public in that such items of information about most of us are publicly available. There might be considerable room for argument as to what should be included on a list of items of such biographical information. Our own suggestion is that the list should include the following:

— full name (including change of name);

— address (including changes of address);

— phone number;

— date and place of birth;

— occupation;

— physical description.

We think that biographical information restricted to the items listed above should be accessible by a security intelligence agency through a system of administrative control similar to that provided for under section 8(2)(e) of the

[37] U.S. Senate, *Final Report of the Select Committee to Study Governmental Operations*, 1976, Book II, p. 329.

proposed Privacy Act. Under the general system for controlling security intelligence investigation that we proposed in Section B of this chapter, the security intelligence agency could make requests to government departments for this kind of biographical data in a Level Two investigation which can be initiated with no higher approval than the Headquarters of the security intelligence agency. However, access to more personal information, including information about a person's financial background, marital history, travel plans, social welfare benefits or employment history, should require a higher level of approval. Obtaining information of this kind can involve an intrusion of a person's privacy as serious as the intrusion involved in electronic surveillance, searches of premises or property, or mail-opening, and should be subject to as rigorous a system of control and review.

**170.** The proposed Privacy Act does not provide a satisfactory test or definition of the national security needs which may justify access to personal information in government files. Section 8(2)(e) would permit access "for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation". The first of these purposes, the enforcement of any law, is reasonably clear (although we note in passing that it establishes that an extremely minor case — for instance, the investigation of a traffic offence — may justify access to very personal information. We will examine this aspect of the legislation in Part X, where we consider legislative proposals related to the criminal investigation responsibilities of the R.C.M.P.). But the second purpose, "carrying out a lawful investigation", presumably for some purpose other than law enforcement, is not at all clear. We think it is a mistake to provide statutory authorization for security intelligence gathering in such vague terms. If statutory provision is to be made for the security intelligence agency's access to personal information in government data banks, it should be tied to a statutory definition of the purpose and scope of security intelligence investigations. Further we think that the statutory definition which is used should provide greater assurance than do existing definitions of subversive activities, including the definition contained in the proposed Privacy Act, that security intelligence investigations will not encroach on legitimate forms of political dissent. Therefore we recommend that access to personal information of both the biographical and more personal kind held by federal government departments and institutions, be accessible for security intelligence purposes only if the investigation falls within the statutory mandate of a security intelligence agency which we have recommended earlier in this Report.

**171.** As we have indicated, we think that requests by the security intelligence agency for personal information, beyond 'biographical information', should require a stricter method of control than that provided in the proposed legislation. Requesting additional personal information from federal government institutions of any kind should be treated as a component of a "full" investigation, the initiation of which, under the general scheme we proposed in Section B above, requires the approval of the Solicitor General. Further, personal information beyond biographical data should be accessible only through a warrant issued by a Federal Court Judge in response to an application of the Director General approved by the Solicitor General of

Canada. The issuance of the warrant should be conditional on meeting the same test of necessity we have recommended for applications for warrants for electronic surveillance, searches and mail examinations. The provision in the proposed legislation for a review by the Privacy Commissioner falls far short of an acceptable means of controlling such a potentially intrusive technique of investigation. Not only is that latter system confined to *ex post facto* review, but, under it, the Privacy Commissioner would not be informed of each instance in which access to personal information was granted. She would review only those cases where she requested a copy of the security agency's application. How is she to know when a questionable application has been made? She can also review complainants' allegations of improper disclosure: however, as we have repeatedly emphasized, it is of the essence of security intelligence investigations that the subjects of such investigations be unaware of the investigation. It is precisely for that reason that we believe a system of prior approval, involving the judicious application of a strict test of necessity, is needed as a means of ensuring that government information about the personal details of one's private life, beyond those items that are generally public knowledge, is used for national security purposes only when a clear case for the necessity of such use has been made.

**172.** If the scheme we recommend were to be adopted, review by the Privacy Commissioner might be retained to enable that official to carry out her general function of monitoring the protection of privacy in government institutions. But, in addition, provision should be made for the review of warrants for use in the security intelligence agency similar to that recommended for the review of other warrants authorizing the use of extraordinary investigatory powers by the security intelligence agency — i.e. Parliamentary review and review by the Advisory Council on Security and Intelligence.

**173.** Warrants granting access to personal information should be submitted to the Minister of the Department or head of the institution which possesses the information. The question arises whether the Minister or head of the institution should have discretion to refuse to accede to a request authorized by warrant. Situations may arise in which a Minister believes that the integrity of a programme administered by his Department is seriously jeopardized by the disclosure of personal information obtained with an expectation of confidentiality. We have considered this matter carefully and have concluded that, providing that the warrant has been granted on the basis of a showing of necessity according to the procedures we have recommended, the head of the institution receiving the warrant should not have discretion to refuse to comply with the terms of the warrant. If the Minister or head believes that a particular warrant is unreasonable, or that a series of warrants indicates excessive use of his institution's records and is unable to persuade the Solicitor General to withdraw the warrant, he could make representations to the Prime Minister and ask that the Solicitor General be directed by the Prime Minister not to execute the warrant. But if the necessity of obtaining information for the protection of national security has been determined by the Minister responsible for the security agency and according to a reasonably precise statutory standard applied by a judge, then we do not think it right to leave it to another

Minister or head of an institution to put the requirements of his Department ahead of the requirements of national security. The Prime Minister or Cabinet might decide that the integrity of some other government programme should be given more weight than protection against a particular threat to national security, but this determination of priorities should not be left to a Minister or head of an institution who has no personal responsibility for national security matters.

*Personal information held by provincial governments*

**174.** There are a number of kinds of personal information held by provincial governments or institutions under provincial jurisdiction which are useful to a security intelligence agency. In the past the R.C.M.P. Security Service has used information from the following provincial or municipal sources:

- hospital and health insurance records
- vital statistics records
- land titles records
- motor vehicle and driver's licenses
- retail tax records
- education records
- welfare records
- public utilities records
- electoral records

As we reported in Part III, information from these sources sometimes was obtained in ways not authorized or provided for by law. While we have no doubt about the security intelligence agency's need to obtain certain kinds of personal information from government institutions under provincial jurisdiction, we believe, that, with one possible exception, the legally authorized means of access which now exist are adequate and that there is no need to seek the support of the provinces for legislative amendments in this regard.

**175.** It is extremely important that the security intelligence agency be directed to obtain information from officials who are authorized by law to release the information and not through undercover sources. If a legally authorized means of access is not available with respect to some category of provincial information which the security agency considers essential, the matter should be raised with the Solicitor General of Canada and, if he is persuaded of the need for the information in question, he should seek the co-operation of the appropriate provincial Minister in making arrangements for a legal method of access. If the provinces adopt privacy legislation which restricts access to personal information as strictly as does Part IV of the Canadian Human Rights Act, then it may well be necessary to seek provincial support for an exception to such restrictions which would permit access by the security intelligence agency on terms similar to those we have recommended should apply at the federal level.

**176.** The one qualification we make to our judgment that there is no immediate need for provincial legislative change permitting security intelligence agency access to provincial government information concerns hospital and medical insurance records. As Commissioners who have had an opportunity to study national security needs, we think that we should report our findings as to the problem that existing statutory restrictions create for a security intelligence agency. Briefly, we can report that situations have arisen in the past in which information from hospital or health insurance records has been of great assistance in successfully completing investigations of persons whose activity has constituted a significant threat to the security of Canada. For example, information obtained from the details of an individual's medical history was crucial in a major counter-espionage investigation. Psychiatric information has been of importance in providing security intelligence advice to those responsible for coping with terrorist situations. We think it is likely that similar situations will arise in the future in which detailed medical information will be of great assistance in the successful completion of important security investigations. Although we have been able to examine only a sample of the legislation which governs access to medical and health records in the various provinces, we note that there are secrecy provisions in the statutes and regulations of a number of provinces which would clearly bar access by a security intelligence agency to confidential information for purposes other than the enforcement of the Hospital or Insurance Act itself. In these provinces, the statutory provisions do not permit even the Minister, Hospital Board or Insurance Commission to authorize release of medical records for security intelligence investigations.[38]

**177.** We think the infrequent but relatively urgent security investigation needs create the strongest case for providing some lawful means of access to medical and health information by a security intelligence agency. (As we noted earlier, we comment on this matter in more detail in Annex I where we examine the relevant recommendations of the Krever Commission.) Hospital and medical insurance records are also useful sources of biographical data in identifying and locating individuals. But we think the need for access to biographical information through hospital or medical records may be significantly reduced if the legal barriers to obtaining such information at the federal level are modified along the lines recommended above and provided for in legislation now before Parliament. Also we should note that, if the changes in the security screening procedures which we recommend in Part VII of this

[38] We examined secrecy provisions in the following Acts:

Alberta Health Care Insurance Act, Saskatchewan Medical Care Insurance Act, Ontario Health Insurance Act, Nova Scotia Hospitals Act, Nova Scotia Health Services and Insurance Act, P.E.I. Health Services Payment Act, Newfoundland Medical Care Insurance Act, Saskatchewan Hospital Standards Act, Newfoundland Medical Care Insurance Act. One statute relating to medical and health information which has no confidentiality or secrecy provisions is the British Columbia Medical Services Act (S.B.C. 1967, ch.24).

Report are adopted, there will be no need for the security intelligence agency to have access to medical information in carrying out its responsibilities in the security clearance process. If a government department considers that it needs medical information, for instance a record of a person's psychiatric treatment, in order to assess an individual's 'reliability' for a security sensitive position, under our proposals it would have to obtain that information with the individual's consent through security staffing officers in the department or from the Public Service Commission. Under our proposals, such information is not to be obtained, either openly or surreptitiously, through the security intelligence agency.

**WE RECOMMEND THAT legislation authorize the heads of federal government institutions to release information concerning an individual's name, address, phone number, date and place of birth, occupation and physical description on receiving a written request from the security intelligence agency stating that such information is necessary for the purpose of locating or identifying an individual suspected of participating in one of the activities identified as a threat to the security of Canada in the statute governing the security intelligence agency, and that all other personal information held by the federal government, with the exception of census information held by Statistics Canada, be accessible to the security intelligence agency through a system of judicially granted warrants issued subject to the same terms and conditions and system of review as recommended for electronic surveillance, searches of premises and property, and the examination of mail.**

**(25)**

**WE RECOMMEND THAT warrants issued for obtaining personal information for security intelligence purposes be submitted to the Minister or head of the government institution which holds the information and that the Minister be required to comply with the warrant unless the Prime Minister directs the Solicitor General not to execute the warrant.**

**(26)**

**WE RECOMMEND THAT the security intelligence agency obtain personal information held by government institutions under the jurisdiction of provincial governments only from persons legally authorized to release such information and that, with regard to any province in which there is no authorized means of access to information to which the Solicitor General of Canada considers that the security intelligence agency should have access in order to discharge its responsibilities effectively, the Solicitor General should seek the co-operation of the province in amending its laws to make such access possible.**

**(27)**

## I. THE WARRANT SYSTEM AND PROPOSED LEGISLATION

**178.** We conclude this chapter by explaining how the various warrants we have recommended for the use of extraordinary investigative methods by a

security intelligence agency should be related to one another and by setting out a draft legislative basis for this warrant system.

**179.** Our recommendations would make the security intelligence agency's use of four extraordinary powers conditional on obtaining a warrant from a Federal Court Judge. These four powers are the interception of communications by electronic surveillance, searches of private premises or property in circumstances in which a search warrant for criminal investigation would not be available, the examination of mail, and access to personal information other than 'biographical information' held by the federal government. We refer to these powers as 'extraordinary' because they involve acts which would be violations of law if carried out by ordinary citizens, and because, unlike special police powers, they may be exercised in circumstances where there is no evidence that a particular crime has been committed or is about to be committed. Two other techniques, which are not extraordinary in this sense, namely surveillance of private premises by hidden optical devices or cameras and the use of dial digit recorders, should also be subject to this system of control by judicial warrants.

**180.** Under our recommendations for controlling the level of investigation, the security intelligence agency could not initiate a request for a warrant to use any of these techniques to gather intelligence about a specific individual or group until a 'full' investigation of that individual or group has been approved. It will be recalled that a decision to carry out a full investigation must be approved by the Solicitor General on a proposal which is supported by the Director General and has been carefully reviewed by a Committee which includes senior officers of the security agency as well as a lawyer from the Department of Justice and a senior official of the Solicitor General's Department. At the time the Solicitor General's approval of a full investigation is sought, the security agency might request his approval of an application to a judge for a warrant for a particular technique. It might conceivably at that time request his approval for applications for warrants for more than one technique, but in this case it would be extremely important for the security agency and the Solicitor General to give careful consideration to the necessity of using each technique. Every effort should be made to use only that method which is best calculated to enable the agency to complete an investigation with a minimum intrusion of privacy. We do not think that the various techniques requiring a judicial warrant can be scaled in terms of their inherent intrusiveness. Indeed, in some circumstances, the use of an undercover informant, which does not require a judicial warrant, may be regarded as a more intrusive and less effective means of obtaining information than one of the techniques which does.

**181.** In considering an application for a warrant to use two or more methods, the Federal Court Judge would have to consider the strength of the case which is made for the necessity of using each technique. He should also be informed, when considering any application, whether warrants have been issued for the use of other techniques in relation to the same subject of investigation and, if they have, what results they have produced. It is essential that the judge be in a position to consider whether, given what has been obtained or what can

reasonably be expected to be obtained from other techniques, and given the statutory direction to minimize intrusions on privacy, the necessity of using a particular technique has been demonstrated.

**182.** Finally, an important focal point in the review of the warrant process carried out by the Parliamentary Committee and the Advisory Council on Security and Intelligence would be the extent to which the various warrants are used together. Indications that warrants were being applied for and obtained on a 'blanket' basis would justify a critical re-examination of the system.

**183.** The system of judicial warrants we have proposed would require the repeal of section 16 of the Official Secrets Act and its replacement by provisions of the statute governing the security intelligence agency. We have set out below a draft of the legislative provisions we envisage for this purpose.

*Proposed Section of the National Security Act*

(1) In this section,

(a) "interception" includes listening to, recording or acquiring any communication, any written communication other than a message in the course of post, and any telecommunication, and acquiring the substance, meaning or purport thereof;

(b) "premises" includes any land, place, vehicle, trailer, mobile home, vessel or aircraft.

(2) Upon the application of the Director General of the Security Intelligence Agency approved in writing by the Solicitor General of Canada, a designated judge of the Federal Court of Canada may issue a warrant authorizing one or more of the following:

(a) the interception or seizure of any communication, other than a message in the course of post, by the use of an electromagnetic, acoustic, mechanical or other device;

(b) the interception or seizure from any person having, in the ordinary course of business, custody of the original copy, record or transcript of any communication, other than a message in the course of post;

(c) the operation of a concealed optical device or camera in a place to which the public does not have access;

(d) the use of a dial digit recorder;

(e) in respect of an article of mail in the course of post, an examination of its exterior, photographing of its exterior, or its opening and the examination and copying of its contents;

(f) the inspection of any premises and of any specified thing or things generally to be found in the premises, and the photographing or copying of the thing or things;

(g) access to personal information (other than biographical information as defined in this Act) under the control of government institutions.

(3) Before issuing a warrant under subsection (2) the judge must be satisfied by evidence on oath that the procedure authorized is necessary for the prevention or detection of any of the following activities:

(a) activities directed to or in support of the commission of acts of espionage or sabotage ('espionage' and 'sabotage' to be given the meaning of the offences defined in sections 46(2)(b) and 52 of the Criminal Code and section 3 of the Official Secrets Act);

(b) foreign interference, meaning clandestine or deceptive action taken by or on behalf of a foreign power in Canada to promote the interests of a foreign power;

(c) political violence and terrorism, meaning activities in Canada directed towards or in support of the threat or use of serious acts of violence against persons or property for the purpose of achieving a political objective in Canada or in a foreign country.

(4) An applicant for a warrant must disclose to the judge before whom the application is brought the details of any application made previously with respect to the same matter.

(5) In deciding whether the procedure for which such authorization is applied for is necessary for the prevention or detection of any such activity, the judge shall take the following factors into consideration:

(a) whether other investigative procedures not requiring a judicial warrant have been tried and have failed;

(b) whether other investigative procedures are unlikely to succeed;

(c) whether the urgency of the matter is such that it would be impractical to carry out the investigation of the matter using only other investigative procedures;

(d) whether, without the use of the procedure it is likely that intelligence of importance in regard to such activity will remain unavailable;

(e) the value of the intelligence product obtained from any warrants previously issued pursuant to this Act in relation to the same subject of investigation;

(f) whether the degree of intrusion into the privacy of those affected by the procedure is justified by the value of the intelligence product sought;

(g) such other circumstances as may be relevant.

(6) The Director General of the Security Intelligence Agency may, with the written approval of the Solicitor General, appeal a refusal of a judge to grant a warrant to the Federal Court of Appeal.

(7) In emergency situations where, in the opinion of the Solicitor General of Canada, the time required to bring an application before a judge would result in the loss of information necessary for the protection of the security of Canada, the Solicitor General of Canada may issue a warrant to the Director General authorizing the use of one or more of the procedures listed in subsection (2) for a period of 48 hours, provided that he is satisfied by evidence on oath that it is necessary for the purposes set out in subsection (3) and provided that the warrant is subject to the same terms and conditions other than the maximum time periods that would apply if a warrant for the same purpose was issued under subsection (2). The Advisory Council on Security and Intelligence must be notified whenever a warrant is issued under this subsection.

(8) A warrant issued pursuant to subsection (2) or subsection (7) shall be issued to the Director General and those persons who act upon his direction or with his authority and

(a) in the case of a communication, shall specify the type of communication to be intercepted or seized;

(b) in all cases, shall state the activity referred to in subsection (2) in respect of which the warrant has been applied for;

(c) in all cases, shall specify the length of time for which the warrant is in force, which shall not exceed 180 days;

(d) in all cases, the judge by whom the warrant is issued or the Solicitor General issuing a warrant under subsection (7) shall include therein such terms and conditions as he considers appropriate, including such powers as are provided for in subsection (9) and are appropriate in order to enable the procedure to be effected without the knowledge of any unauthorized person.

(9) A warrant issued pursuant to subsection (2) or subsection (7) may provide that in the case of the procedures referred to in (a), (b), and (f) of subsection (2) the persons carrying out the procedure may take such steps as are reasonably necessary to enable them

(a) to install any device the use of which is authorized;

(b) to monitor, repair and remove the device;

(c) to enter premises for the purpose of

(i) examining the premises prior to installation of the device;

(ii) installing the device;

(iii) monitoring, repairing and removing the device;

(d) to operate the device by using the electrical power supply that is available in the premises;

(e) to copy material;

(f) to examine the contents of receptacles, including luggage;

(g) to take such other steps as may be reasonably necessary for such purpose,

provided always that in all these cases

(h) any such steps shall cause no significant damage to the premises that remains unrepaired; and

(i) in no case shall the persons carrying out the procedure use physical force or the threat of such force against any other person; and

(j) in every case the persons carrying out the procedure shall be accompanied by a peace officer.

(10) (a) The Postmaster General of Canada shall be notified whenever a warrant is issued pursuant to subsection (2) or subsection (7) authorizing use of the procedure referred to in (e) of subsection (2), and Canada Post shall give to persons acting in pursuance of such a warrant all reasonable assistance.

(b) A warrant issued pursuant to subsection (2) or subsection (7) may provide that in the case of the procedures referred to in (e) of

subsection (2) the persons carrying out the procedure may remove the article of mail from the course of post and even from the post office but only as long as is reasonably necessary to enable the procedure which is authorized to be carried out.

(c) The procedure authorized by such a warrant may be carried out notwithstanding the provisions of section 43 of the Post Office Act and without any person thereunto duly authorized committing any offence under that Act.

(11) Warrants issued pursuant to subsection (2) and subsection (7) authorizing the use of the procedure referred to in (g) of subsection (2) shall be submitted to the head of the government institution which controls the information which is requested and the head of the institution shall direct that the information requested be disclosed according to the terms specified in the warrant.

(12) A renewal of the warrant may be given if the judge to whom an application for the renewal is made is satisfied that, if the application were for a warrant, he would have issued it pursuant to subsection (2), and, in addition to the requirements of subsections 3, 4 and 5, he shall be provided with evidence under oath as to the intelligence obtained pursuant to the warrant.

(13) The Solicitor General of Canada shall, as soon as possible after the end of each year, prepare

(a) a statistical report to be laid before Parliament setting forth

(i) the number of warrants issued for each of the procedures referred to in (a) to (g) of subsection (2);

(ii) the number of warrants issued which were renewals of warrants previously granted;

(iii) the extent to which warrants have been renewed more than once.

(b) a report to be presented for examination by the Joint Committee of Parliament on Security and Intelligence providing

(i) an assessment of the value of the intelligence products resulting from the use of warrants issued under subsection (2);

(ii) an account of any difficulties encountered in the administration of this section which might indicate the need for amendments to the section.

(14) Section 178.11(1) of the Criminal Code shall not apply to

(a) a person who intercepts a private communication as defined in section 178.1 in accordance with a warrant issued pursuant to subsection (2);

(b) any person who in good faith aids in any way a person who he has reasonable and probable grounds to believe is acting under the authority of any such warrant.

(15) Section 178.18(1) of the Criminal Code shall not apply to a person in possession of a device such as is referred to therein for the purpose of using it in an interception made or to be made in accordance with a warrant issued pursuant to subsection (2).

(16) Section 178.2(1) of the Criminal Code shall not apply to a person who discloses a private communication, as defined in section 178.1 of

the Criminal Code, or any part thereof or the substance, meaning or purport thereof or of any part thereof, or who discloses the existence of a private communication for any purpose within the scope of the power of the security intelligence agency, or for any purpose of review of the operation of this section exercisable pursuant to this Act by the Advisory Council on Security and Intelligence and the Parliamentary Committee on Security and Intelligence.

(17) No action lies under Part I.1 of the Crown Liability Act in respect of any procedure carried out pursuant to a warrant issued under subsection (2).

(Section 16 of the Official Secrets Act would be repealed. The new section should provide for the continuation in effect of all warrants issued under section 16 of the Official Secrets Act for 30 days after the coming into effect of the section, as if they had been authorized by a warrant issued by a judge pursuant to the new section.)

(Section 178 of the Criminal Code should be amended wherever necessary to ensure that an interception under a warrant is on the same plane as one pursuant to a section 178 authorization: e.g. to ensure that there is no question about the admissibility of the intercepted private communication in evidence in a judicial proceeding.)

# CHAPTER 5

# ANALYSIS, REPORTING, AND ADVISING FUNCTIONS

## INTRODUCTION

**1.** In previous chapters in this part of our Report, we established criteria for deciding the proper subjects or targets of a security intelligence agency's investigative activities. We also described the methods that the agency can employ to collect information about these targets, and the controls necessary to ensure that the risk to Canada's security justifies the use of the more intrusive means of gathering information. In this chapter, we focus on what the agency should do with the information it collects. We begin with the analysis function by examining the purposes of analysis and the current strengths and weaknesses of the Security Service's analytical capabilities. Our recommendations for improving this function then follow. A fundamental theme throughout this section is our belief that analysis is of prime importance for a security intelligence agency which is effective and which acts within the law. Indeed, it is not an exaggeration to say that analysis has a dominant effect on all of the significant activities that such an agency performs.

**2.** From analysis, we turn to the agency's reporting and advising functions. We begin by developing basic principles in regard to two matters: first, what the agency should report and advise on, and second, to whom it should report and give advice. We then describe the nature of the reporting and advising programmes that a security intelligence agency should adopt and conclude with recommendations on the type of controls which should govern the reporting function.

## A. ANALYSIS

*The importance of analysis*

**3.** Those familiar with security or intelligence agencies often describe the work of these organizations in terms of four functions: targetting, collecting, analyzing, and dissemination (Vol. 69, pp. 11180-82). We have found this description useful for some purposes, including the structuring of this part of our Report. Nevertheless, the simplicity of this description, though one of its attractive features, may lead to difficulties if it is used as a basis for drawing important conclusions about organizing the government's security intelligence functions. For example, to conclude that any of the four functions is a separate

component which can be neatly detached from the others and placed in a separate organization would be a serious misjudgment.

**4.** That is why we disagree with Commissioner Simmonds, who, in his testimony before us, suggested that the R.C.M.P. Security Service should become essentially a collection agency, and that primary responsibilities for analysis should lie elsewhere in government:

> . . . if for the future we take a look at a different way, in broad terms, of Government organization to handle security matters, then it seems to me that the role of the Service within the Force should be mostly one of just investigating and collecting intelligence and so on and doing low level analysis, but some of the things we, perhaps, have been expected to do, be done in another forum.
>
> (Vol. 165, p. 25377.)

The most compelling reason for rejection of that opinion is that a security intelligence agency cannot do the targetting and collecting functions properly and effectively without a well-developed analytical capability. The judgments involved in the targetting process are difficult. When, for example, does proper diplomatic behaviour shade into foreign interference? What forms of political violence are properly the concern of a security intelligence agency in addition to being the concerns of local and provincial police forces? What is the difference between 'revolutionary subversion' and dissent? Such judgments should be based on more than 'low level' analysis.

**5.** There is a similar need for sound analytical skills in directing the agency's investigative work. Those in senior operational roles are required to make important choices daily about the allocation of the agency's limited investigative resources: whether, for instance, physical surveillance teams should follow target A or target B to ensure the likelihood of the bigger payoff, and when it is appropriate to use other investigative tools, including electronic surveillance and informants. After information about a target is collected, agency personnel must analyze it so as to redirect investigative efforts if necessary. This type of analysis involves the piecing together of scraps of information to produce a working hypothesis about the intentions and plans of the target. Intuition, experience in the tradecraft of counter-espionage, and knowledge of the target combine with clear logical analysis to produce expertise in this area. Without such expertise, a security intelligence agency cannot possibly be successful in its investigative work.

**6.** Analysis plays a key role in the agency's reporting function. Raw information about possible threats to security will be of little value to government unless the significance of that information is explained clearly. Crucial to this reporting function is the capacity of agency personnel to undertake research using books, articles and reports on all subjects related to the social, economic, and political processes — national and international — relevant to the security of Canada. This research is important not only in writing reports to government but in distinguishing between those activities which require surveillance and those which do not.

**7.** Another argument bolsters our conclusions about the importance of analysis to a security intelligence agency. Any other department or agency would have difficulty in getting access to the kind of information collected by the security agency, and therefore would have difficulty in attempting analysis. In evidence before us, Mr. Robin Bourne, the former head of the Police and Security Planning Branch in the Solicitor General's Department, made this point as follows:

> The first problem was the whole business of the need-to-know information and protecting third party interests. Obviously, long-term research into these kinds of subjects would not be effective, unless we had all the information that was available to do this kind of research. There is no question that we were not getting from the R.C.M.P., which was the prime source, all the information which we needed to have for that kind of research... and there were very good reasons for that...
>
> Everyone is suspect in the security business until they prove themselves otherwise. We hadn't really had time to prove ourselves. So, we really did not have the basic information to do the research... I think you will find that throughout the world, most security services and intelligence organizations do have as an integral part of their organization, the research branch, just for that reason. So that they do have free access to the information.
>
> (Vol. C68, pp. 9471-73.)

With regard to Mr. Bourne's first point, our examination of the R.C.M.P. files concerning the relationship between the Security Planning and Analysis Research Group (SPARG) and the Security Service satisfies us that the Security Service will vigorously resist any proposed arrangement that would involve outside analysts having access to Security Service files.

**8.** To recognize the importance of analysis, the security intelligence agency's analytical responsibilities should be stated explicitly in the statute establishing the agency. This is not to argue that the analysis function should reside exclusively with the security intelligence agency. Rather, a number of agencies should have skills in this area. The question then becomes how these skills are co-ordinated at the centre of government to be of maximum benefit to Ministers and senior government officials. We shall return to this question in Part VIII of this Report, where we discuss the security and intelligence co-ordination mechanisms at the centre of government.

*Assessing the Security Service's analytical capacity*

**9.** The Royal Commission on Security in 1969 was critical of the Security Service's capacity to provide government with clear, timely, useful information about security threats facing Canada.

> 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 R.C.M.P. 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 policymaking levels. A specific area in which the effectiveness of the

R.C.M.P. does appear to us to be capable of improvement involves personnel investigations.[1]

**10.** Our own research — based on interviews with Security Service personnel and the primary consumers of Security Service intelligence reports in other government departments, and based on a thorough study of a cross-section of Security Service reports — leads us to conclude that, while there has been some improvement since the Royal Commission on Security, the Service still has serious deficiencies in this area. One of our findings is that the Security Service's reports and assessments are heavily oriented to providing covertly collected information about specific groups and individuals. Many departments which receive these reports have found them useful and have complimented the Service on its investigative skills. Reaction to Security Service products, however, has been by no means uniform. Officials of several departments have been highly critical, voicing two common complaints: Security Service personnel lack experience and knowledge about what constitutes legitimate diplomatic behaviour, and they do not know enough about government — how it works and the needs of Ministers. Our review of Security Service reports confirmed the validity of these criticisms, and indeed, many within the Security Service agree with them. We, as a Commission, add an additional concern. Some of the analysis done by the Security Service demonstrates a serious inability to distinguish between agitators for social change and those who pose a significant threat to Canada's democratic process of government. Examples of this tendency occurred in the work done on the Extra Parliamentary Opposition (E.P.O.), and in the analysis leading up to the countering operations in the early 1970s (Operation Checkmate).

**11.** The Security Service is weakest when it comes to analysis which is longer term, more broadly based, and less oriented to specific groups and individuals. Such analysis, which tends to rely on both overt and covert sources of information, is often called 'strategic' analysis. The Security Service does not do enough of this type of analysis and what it does is not of high quality. In voicing this criticism we are not arguing that the Security Service lacks potential in this area: we have met a number of Security Service staff with well-developed analytical talents. The problem is that there are not enough of them and, in addition, those in middle management often lack the skills and experience to supervise them properly.

**12.** Some Security Service members have argued vigorously that strategic analysis is not within their mandate: they have not been asked by government to perform this function. We believe that such an argument is based on too narrow an interpretation of the Security Service's mandate. The argument is also suspect in that the Security Service has, on occasion, done just this broader based, longer term type of analysis. The chief reason why the Security Service does so little of this type of analysis, in our view, is that its members do not feel confident about their capacity for doing it. As a result, Security Service products are often unbalanced, relying far too much on covertly collected information, and not nearly enough on what is available through overt means.

---

[1] *The Report of the Royal Commission on Security*, paragraph 56.

*Proposals to strengthen the analytical function*

**13.** Our proposals for strengthening the analytical capabilities of Canada's security intelligence agency fall into three categories. First, we shall recommend in Part VI, Chapter 2, that the agency be staffed with individuals who are well-educated in a variety of disciplines, who express themselves clearly, who have in many instances working experience in other organizations before joining the agency and who are full members eligible for promotion to senior positions. Similarly, the agency requires senior and middle level managers who can select, develop, and direct a highly versatile and well-educated staff. Second, in Part VIII, Chapter 1, we shall recommend a revamped and revitalized interdepartmental committee system, which will allow the consumers of the agency's products to play a more active role in setting the government's intelligence collection priorities and in providing the collecting agencies with better assessments of the strengths and weaknesses of their current products. Third, also in Part VIII, Chapter 1, we shall recommend that the government establish a central Bureau of Intelligence Assessments to provide intelligence estimates derived from the products of collecting agencies and from public sources of information. Such a bureau, we believe, should develop a small but highly expert staff to serve, in part, as a stimulus to other security and intelligence agencies within government to improve the quality of their analyses. In addition to these proposals, we shall put forward, as a suggestion only, an organizing approach to ensure that those specializing in analysis within the security intellligence agency are used with most benefit. We now turn to this suggestion.

**14.** On two separate occasions in the past, the Security Service established a specific unit, separate from the operational branches, with the resources and responsibility for doing research and analysis. The disadvantage has been that such a unit tends to get cut off from the operational branches. 'Hardnosed' operational personnel view these intellectually oriented researchers with suspicion, are reluctant to share their most sensitive information with them, and resent having their conclusions 'reworked' by a group without any current operational know-how. The result is that the separate research group works primarily on peripheral matters, and the overall quality of analysis has not been improved to any degree. Another solution, which the Security Service has also tried, is to establish separate analytical units within each operational branch. The risk in this approach is that these units will focus entirely on high priority operational problems and have little time for more in-depth contextual analysis and research.

**15.** One way out of this dilemma which we believe worthy of consideration is to establish a small research group which does not formally report to any of the operational branches but is available to them as a centralized service. Operational branches would retain responsibility for producing major pieces of analysis (requests for these papers would likely come from interdepartmental committees or the senior management of the agency), and would second researchers and writers for short periods from this central pool to work with their operational people for this purpose. Such temporary working groups within the agency would bring together the writing skills and familiarity with

overt sources which the centralized pool of researchers would possess, with the 'street' knowledge and access to covert sources of information which are the forte of those in operational branches.

**WE RECOMMEND THAT the security intelligence agency's responsibilities for the development of a competent analytical capability be explicitly stated in the statute establishing the agency.**

(28)

## B. REPORTING AND ADVISING

*Basic principles*

**16.** The reporting of timely, cogent information about security threats facing Canada is the *raison d'être* of a security intelligence agency. The word "dissemination" is often used by those working in security and intelligence organizations as a convenient label for this function, but we prefer the term "reporting". "Disseminate", according to The Concise Oxford Dictionary, means "scatter about, sow in various places". In our examination of Security Service reporting activities, we have found evidence of numerous problems stemming from poor judgment concerning both what the Security Service reports and to whom. In our view, there should be no indiscriminate spreading of security intelligence information, especially information relating to individuals and groups. For this reason, we prefer to use the word "reporting".

**17.** Given the importance of the reporting function, it should be provided for in the Act establishing the agency. In addition, the Act should state that limits must be applied to this reporting function in the form of instructions or guidelines issued by the Minister responsible for the security intelligence agency. These guidelines should be approved by the Cabinet Committee on Security and Intelligence and reported to the Joint Parliamentary Committee. We briefly set out here a number of principles on which these guidelines should be based.

**18.** The first of these principles is that the security intelligence agency, with few exceptions, should report only information relevant to threats to security as those threats have been defined by Parliament. The agency should not report information which names individuals or groups, unless such information can reasonably be related to some activity threatening the security of Canada. Information concerning individuals should be reported only to departments which require it for security clearance purposes or to departments, Ministers, police forces or foreign agencies who need the information because of their recognized responsibilities to deal with security threats as defined by the Canadian Parliament. In Chapter 7 of this Part we shall discuss the types of problems which a security intelligence agency can encounter in reporting information to foreign agencies. We shall also suggest control procedures for governing this activity.

**19.** In enunciating the above principle, we have purposely inserted the qualifying phrase "with few exceptions". This qualification is meant to cover those few cases where the security intelligence agency, in the course of

investigating a threat to security as defined by Parliament, *accidentally* comes across information unrelated to the security of Canada which it should report to a domestic police force, or to a provincial government or to the federal government. For example, in its investigations of a domestic group suspected of plotting some terrorist act, the security intelligence agency may stumble upon information about activities which, though criminal, are unrelated to national security. We believe that the security intelligence agency must report such information to the appropriate police force. If the agency believes that to report such information would likely be detrimental to the security of Canada, full details of the matter should be reported immediately to the Solicitor General, for his decision as to whether or not the information ought to be reported. While we think it desirable that the Solicitor General should consult with the Attorney General of Canada at this stage, he should not be obliged to do so if he believes that the information ought to be released to the police. On the other hand, if the Solicitor General agrees that the security of Canada would be adversely affected by reporting the matter to the police, he should refer all the details to the Attorney General of Canada for his decision as to whether the interests of the security of Canada outweigh the interests of the administration of justice. (See discussion in Chapter 8 of this Part.) As a second example, if the security intelligence agency, in its investigation of a suspected foreign intelligence officer, were accidentally to collect information relating to a foreign government's prospective bargaining position on an important trade issue with Canada, we believe it should be able to report such information to the appropriate Federal or Provincial government department.

**20.** We recognize that, in allowing exceptions to the general principle about reporting only security relevant information, we open up a potential for two kinds of abuse. First, if the agency is permitted to report information which it has no mandate to collect, there is a great danger that its collection activities will secretly expand. Second, there is a danger that the agency will report certain accidental by-products which it has no business reporting. For example, it would be highly improper for Cabinet Ministers to receive information about their political opponents from a security intelligence agency. Using the agency in this manner would do irreparable harm to Canada's democratic form of government. Similarly, a security intelligence agency should not report any information it has collected accidentally on the policies or strategy of a provincial government.

**21.** To guard against these potential abuses, we make several proposals. As a first step, the ministerial guidelines on reporting should deal explicitly with the types of accidental by-products of authorized investigations which the security intelligence agency can properly report. Before reporting these by-products, the agency should require ministerial approval. In addition, the security intelligence agency should retain, in one convenient location, records of all accidental by-products reported to government or to the police so that the independent review body has ready access to them. These records should state what information was reported, how the reported information was collected, to whom it was given, and the history of the investigation which produced the information. The independent review body should monitor closely these investi-

gations to ensure that they are not being misdirected for a purpose irrelevant to the security of Canada. Finally, the security intelligence agency should not analyze the accidental by-products, nor should it comment on their significance.

**22.** In addition to elaborating upon the type of information that a security intelligence agency can report, the guidelines issued by the Minister should also make clear to whom the agency can report information. Ministers, both provincial and federal, government departments, police forces, and foreign agencies will be the chief recipients of the products produced by the agency. The agency, however, should not report information on its own initiative directly or indirectly to the news media. As we state in the next chapter on executive and preventive functions, it should not be the responsibility of the agency to publicize threats to security. That function must rest with the Minister responsible for the agency. There should be no contrived 'leaks' by the security intelligence agency nor cultivation of media sources for the purpose of planting articles provided by the agency. Activity of this kind is highly dangerous in that it may involve the agency in attempts to manipulate the media.

**23.** The agency should also exercise great care in reporting information to individuals who are not government officials, Ministers, or police officers. In the chapter which follows, we shall discuss when it is proper for a security intelligence agency to do so.

**24.** There is one additional topic concerning the reporting function which we wish to address. That focusses on the caution practised by a security intelligence agency in revealing the sources on which its intelligence judgments are based. Policymakers can find such caution frustrating if they wish to know whether the agency's judgments are based on information provided by a strategically placed agent, on inference drawn from diverse pieces of information, or simply on a guess on the part of the agency analysts. On the other hand, an agency's reticence in these matters is not entirely without foundation. Consider the following example documented by an American author writing about the C.I.A.:

> With war raging in Bangladesh between Indian and Pakistani forces in December 1971, evidence began to mount that India was planning an attack on West Pakistan as well. On December 7, Kissinger asked the C.I.A. for an estimate of the probability of such an attack. The C.I.A. said it didn't know. But within twenty-four hours it had positive information: the C.I.A. case officer handling the Indian politician in Gandhi's cabinet in New Delhi was told that a decision had just been reached to attack in the West. A report was immediately cabled back to Langley and forwarded directly to the White House in its raw form. Nixon was later to cite this cable as one of the few really timely pieces of intelligence the C.I.A. had ever given him, but the Agency paid a price. The report was widely read in the White House, and its text, along with many other documents, was quickly leaked to Jack Anderson, who published them in his column in mid-December. That was the end of the agent. According to [a senior C.I.A. intelligence officer], "he told us to go to hell".[2]

[2] Thomas Powers, *The Man Who Kept the Secrets*, New York, Alfred A. Knopf, 1979, pp. 206-207.

**25.** The dilemma described above is not unique to the United States. During interviews conducted by members of our research staff, several officials from 'consumer' departments complained about the Security Service's refusal to divulge its sources. For example, officials from one department cited two occasions when the Security Service attempted to get the Intelligence Advisory Committee's approval for assessments which some members of the Committee strongly suspected came from foreign intelligence services. While this dilemma about revealing sources is not fully resolvable, the security intelligence agency should enter into discussions with consuming departments about how it can best reveal the basis for its judgments while providing reasonable protection for its sources. We believe that a security intelligence agency should be able to provide at least a general idea of the nature of its sources on which a particular report is based, i.e. whether the sources are domestic, foreign, or a combination and the number and reliability of these sources. The Minister responsible for the agency should also address this question in his guidelines on the reporting function.

*Reporting and advising programmes*

**26.** Our review of security intelligence reporting activities has revealed that the Security Service produces a large number of reports. These reports are distributed to a wide variety of consumers from the Prime Minister in some instances to Departmental Security Officers in others. As mentioned earlier, a large majority of these reports tend to be case-oriented, that is, they tend to deal with information collected by covert means about specific groups and individuals. Our recommendations concerning the proper mandate of a security intelligence agency ensure that security intelligence products will continue to be numerous and to be read by a wide variety of consumers. Nonetheless, there should be several important changes. Security intelligence reports should put more emphasis than is now the case on providing government with timely advice on such matters as crisis handling and protective security. In addition, security intelligence reports should be less case-oriented: greater attention should be paid to providing government with longer term, more broadly based assessments of security threats facing Canada. Furthermore, the security intelligence agency's reports to government officials and Ministers about specific groups and individuals should make greater efforts to put this information in context. Thus, a report on the activities of a suspected foreign intelligence officer may need to make clear the difference between acceptable and unacceptable diplomatic behaviour and how the intelligence officer's activities might relate to his country's foreign policy. We will elaborate on these themes further in our discussion of the major security intelligence reporting and advising programmes in the following four areas: screening, emergencies and crises, protective security, and reporting on security threats.

*Security screening*

**27.** Our recommendations for the security intelligence agency's role in security screening — recommendations which we shall develop in Part VII of this Report — call for a significant change in the reporting responsibilities of the agency, especially with regard to screening for government appointments. We

shall propose that the agency no longer have responsibility for doing routine field investigations on all Top Secret clearances. In addition, the agency should report only information on an individual's character which is of direct relevance to security. The effect of these recommendations and others calling for a reduction in Top Secret clearances will dramatically reduce the number of routine reports that the Security Service now provides departmental security officers. However, other recommendations concerning screening for government appointments will increase the agency's advisory responsibilities. For example, we shall recommend that the agency develop a competent research capacity for the purpose of providing advice to government on a variety of matters relating to subornation of public servants, including the following: the latest techniques used by foreign intelligence officers to compromise people; the risks posed by individuals with certain character traits; developments relating to security screening in other countries; and possible policy changes to improve the government's screening procedures. Thus, the changes in screening responsibilities, at least in the public service area, call for a shift away from routine reports on individual cases to more emphasis being placed on providing policy advice to government.

*Emergencies and crises*

**28.** In Part IX, Chapter 1, we shall discuss the role of a security intelligence agency in emergencies and crises. After describing the role played by the Security Service in the 1970 October Crisis, we shall emphasize the importance of the ability of a security intelligence agency to provide opportune, well-written reports which warn governments of potential crises and, in turn, of the capacity of government to digest these reports and react to them. The number as well as the content of such reports calls for careful judgment. Too many reports will lead to officials and Ministers ignoring the agency's advice on these matters. Similarly, the government will lose confidence in the agency if it is too cautious in forewarning about significant political violence. In addition to advising on potential crises, the security intelligence agency should provide government with periodic reports on crisis-handling. The agency should be knowledgeable about the latest trends in international terrorism, the changing nature of terrorist goals and targets, and, among other things, the steps being taken by various foreign governments to counter terrorist threats. In our opinion, the R.C.M.P. Security Service does far too little of this type of reporting to government.

**29.** The agency also has an important reporting role during a particular crisis. It will be responsible for providing the federal government's crisis centre with accurate, up-to-date intelligence reports based on information received from police forces, foreign agencies, and other government departments. Thus, the agency has a filtering function which requires careful judgment and communication skills so that the crisis centre is neither confused by conflicting reports from several sources nor denied an essential piece of information originating from other agencies.

*Advice on protective security*

**30.** A security intelligence agency should be a major source of advice to government departments and police forces which are responsible for enforcing and carrying out measures to protect property and persons from security threats as defined by Parliament. The agency itself should not be assigned the task of actually enforcing or carrying out protective security functions. For example, in airport policing, the agency's role should be to provide information about terrorist threats to airport security officials, to the police and to the Ministry of Transport. In V.I.P. security, the agency should provide intelligence about those who are likely to attack V.I.P.'s for political purposes — their identity, whereabouts and methods. In the vital points programme, the role of the security intelligence agency should be to report on the kinds of situations in which vital points might be attacked by those who fall within the agency's mandate, and on the basis of this analysis, to assist those responsible for the vital points programme in identifying vital points and designing effective security measures. The emphasis in all of these areas, therefore, is on providing useful information and advice, and not on actually carrying out security programmes. Once again, it is our view that the Security Service does not provide government with enough high quality advice on these matters.

*Reporting on security threats*

**31.** Throughout the year, the Security Service provides government with reports on a wide variety of security threats which may not have a direct relationship to screening, preparing for crises, or providing protective security. Some of these reports are provided on a regular basis. For example, the Security Service is required by the 1975 Mandate to report annually to Cabinet. Other reports result from priorities set by an interdepartmental committee. For example, the Intelligence Advisory Committee has, on occasion, requested that the Security Service co-operate with other departments in producing a report canvassing the covert operations in Canada of a particular country. Many of the Security Service's reports, however, result from *ad hoc* requests from departments for information about a particular group, individual, or upcoming event. All such *ad hoc* requests for information from departments or police forces should be drawn to the attention of the agency's headquarters staff to ensure that investigations resulting from these requests are subject to the regular control procedures.

**32.** Earlier in this chapter, we proposed that the agency place more emphasis on providing government with reports on the strategic aspects of security threats facing Canada — how these threats are changing, and the measures government might take to deal with them. In subsequent parts of this Report, we shall make additional recommendations affecting this aspect of the agency's reporting responsibilities. In Part VIII, we shall make proposals for how the agency might improve its annual report to Cabinet. We shall also be recommending that the function of collating and assessing current foreign and security intelligence be consolidated in the Intelligence Advisory Committee. This change will likely affect the current practice of the Security Advisory Committee in preparing and circulating a weekly security intelligence report.

Finally, our recommendation calling for the establishment of a Bureau of Intelligence Assessments should have an important impact on the reporting functions of the security intelligence agency. The agency will find itself responding to many more requests than at present to participate in interdepartmental teams established to assess a variety of longer term security problems facing Canada.

**33.** In conclusion, the recommendations in this Report have important implications for the reporting and advising programmes of a security intelligence agency. Future emphasis will be placed more on providing its consumers with advice and analysis on security problems and less on routine reports dealing with specific individuals and groups.

*Controls on the reporting function*

**34.** We conclude this chapter by summarizing briefly the system of controls which should govern the security intelligence agency's reporting function. This system should consist of at least four parts. The first is the set of guidelines which the Minister responsible for the agency should issue under the authority of the Act creating the agency. The Minister should disclose these guidelines to the Joint Parliamentary Committee. As we noted earlier in this chapter, these guidelines should cover at least the following topics:

— conditions under which the agency can report information about individuals;

— conditions under which the agency can advise individuals outside of governments and police forces about security threats;

— the types of information not relevant to its mandate which the agency, having collected by accident, can report to government;

— the manner in which the agency should handle *ad hoc* requests for information from government departments and police agencies; and

— the manner in which the agency should reveal the basis for its judgments, while at the same time providing reasonable protection for the sources of its information.

We shall also recommend that the Minister responsible for the agency issue guidelines with respect to the agency's relationships with foreign agencies. These guidelines will also be relevant to the agency's reporting function.

**35.** The second aspect of the system of controls governing the reporting function will be the independent review body — the Advisory Council on Security and Intelligence — which we shall recommend in Part VIII. This advisory body will monitor the security intelligence agency's operations including its reporting activities, and in this regard, will be an *ex post facto* control. In performing this function, the Minister's guidelines referred to above will be an invaluable aid in determining those areas of the agency's work which require the Advisory Council's close attention. Complaints by members of the public and by agency employees will be other means whereby this advisory council can direct its investigations.

**36.** Another *ex post facto* control on agency reporting will be the Security Appeals Tribunal which we shall recommend in Part VII. This Tribunal will handle all complaints concerning the federal government's screening activities regarding public servants, immigrants and applicants for Canadian citizenship. Thus, the tribunal will be an important review mechanism for information reported by the agency on individuals.

**37.** A final element in the control system governing the agency's reporting function will be a revamped interdepartmental committee system which we shall recommend in Part VIII. The departments and agencies within the federal government which are the principal customers of intelligence reports have not in the past played a sufficiently active role in the process of setting priorities for those organizations, including the security intelligence agency, which collect and report security and foreign intelligence. A more active group of consumers is essential if the government hopes to achieve value for its money in this area.

**WE RECOMMEND THAT the Act establishing the security intelligence agency specify the reporting function of the agency and require the Minister responsible for the agency to issue guidelines on how the agency should conduct its reporting activities. These guidelines should cover at least the following:**

**(a) conditions under which the agency can report information about individuals;**

**(b) conditions under which the agency can advise individuals outside governments and police forces about security threats;**

**(c) (i) the general principle that the security intelligence agency should report only information relevant to its mandate, except that information which it has collected by accident which the guidelines specifically require or authorize it to report to government or to the police;**

**(ii) the agency should report information which it has collected by accident, which relates to an offence, to the appropriate police force if, in the agency's opinion, to do so would not be likely to affect adversely the security of Canada.**

**(iii) the types of information collected by accident which the security intelligence agency may report to the appropriate federal or provincial government include information pertinent to the economic interests of Canada.**

**(d) the manner in which the agency should handle *ad hoc* requests for information from government departments and police forces;**

**(e) the manner in which the agency should reveal the basis for its judgments, while at the same time providing reasonable protection for the sources of its information.**

**(29)**

**WE RECOMMEND THAT when the Solicitor General receives information from the security intelligence agency relating to the commission of an offence, and the agency considers that it would adversely affect the security of Canada to pass that information to the police, the Solicitor**

**General should consult with the Attorney General of Canada with respect to the release of that information. If, after such consultation, the Solicitor General decides that the security of Canada would not be adversely affected by the release of that information he should instruct the agency to release it to the appropriate police force. On the other hand, if the Solicitor General decides that the release of the information would adversely affect the security of Canada, he should so advise the Attorney General of Canada who should proceed in accordance with arrangements to be worked out with provincial attorneys general. (See discussion in Chapter 8 of this Part.)**

(30)

WE RECOMMEND THAT

**(a) the security intelligence agency retain, in one location, records of all accidental by-products reported to government or to the police, and that such records state what information was reported, how the information was collected, to whom it was given, and the history of the investigation which produced the information; and,**

**(b) the independent review body have access to such records and that it monitor closely the investigations which produced the information to ensure that the investigations are not being misdirected for a purpose irrelevant to the security of Canada.**

(31)

**WE RECOMMEND THAT the agency, in addition to providing information about specific individuals and groups relevant to its mandate, place greater emphasis than is now the case on providing government with:**

**(a) analysis and advice on the latest developments, techniques, and countermeasures relating to physical and V.I.P. security, and security screening; and,**

**(b) reports which analyze broad trends relating to threats to the security of Canada and which advise government on ways to counter these threats.**

(32)

# CHAPTER 6

# EXECUTIVE POWERS AND PREVENTIVE ACTIVITIES

## INTRODUCTION

**1.** Because the essential function of a security intelligence agency is to collect, analyze and report intelligence about threats to Canada's security, we believe it should not be authorized to enforce security measures. Thus, we think the statutory mandate of the agency should not include the functions of "deterring, preventing and countering" which are now included in the 1975 Cabinet Directive defining the Role, Tasks and Methods of the R.C.M.P. Security Service.

**2.** We have two basic reasons for taking this position. First, as we argued in Part III, we think it is unacceptable in Canada that the state should use a secret intelligence agency to inflict harm on Canadian citizens directly. This position, it must be noted, does not prevent a police force or a government department from using intelligence supplied by the security intelligence agency to enforce a law or security measure against an individual. Second, we think the liberty of Canadians would be best protected if measures to ensure security were not enforced by the organization with the prime responsibility for collecting information about threats to that security. The assignment of executive enforcement responsibilities to agencies other than the security intelligence organization assures desirable countervailing powers and avoids the danger that the security intelligence organization might be both judge and executor, in security matters.

**3.** Therefore, we think it would be wise to separate the enforcement function. In this Canada would be following the Australian and New Zealand examples of expressly excluding enforcement functions from the authorized activities of the security intelligence agency. The Australian Security Intelligence Organization Act of 1979 provides that

> 17. (2) It is not a function of the Organization to carry out or enforce measures for security within an authority of the Commonwealth.

Similarly, the New Zealand Intelligence Organization Act 1969 provides that

> 4. (2) It shall not be a function of the Security Intelligence Service to enforce measures for security.

A similar provision should be included in the legislation governing Canada's security intelligence organization.

**WE RECOMMEND THAT the legislation governing the security intelligence agency include a clause which expressly denies the agency any authority to carry out measures to enforce security.**

(33)

## A. POLICE POWERS

**4.** Under the present structure, those members of the Security Service who are regular members of the R.C.M.P. have the powers of peace officers as provided for in section 17(3) of the R.C.M.P. Act. These powers include the powers of arrest and of search and seizure conferred on peace officers by the Criminal Code of Canada, and additional powers conferred by other federal and provincial statutes. In our interviews with members of the Security Service we found that they rarely used their peace officer powers. Nonetheless, the possession of peace officer powers has continued, rather illogically, to be a requirement for management positions in the operational branches of the Security Service, thus posing a barrier to the civilian member's advancement.

**5.** There is no need for peace officer powers in a security intelligence organization which has as its essential function to collect, analyze and report intelligence. On the contrary, in terms of retaining checks and balances in the system, there is real advantage in not bestowing peace officer powers on its members. That is one reason why, in the previous chapter, we recommended that when members of the security intelligence organization exercise investigative powers involving the surreptitious entry of private premises or removal of private property, they should always be accompanied by a policeman who would deal with any breaches of the peace which may occur if the operation were to be suddenly interrupted. The definition of 'peace officer' in the Criminal Code is very wide and besides mayors, reeves, sheriffs, justices of the peace, wardens, prison guards, police officers, constables and bailiffs includes "... other person employed for the preservation and maintenance of the public peace...".[1] To remove any doubts, the statute governing the security intelligence organization should explicitly state that members of the organization are not to be considered peace officers.

**WE RECOMMEND THAT members of the security intelligence agency should not have peace officer powers and that, to remove any doubt, the legislation establishing the organization should explicitly state that members of the security intelligence organization are not to be considered as peace officers.**

(34)

## B. PERMISSIBLE AND IMPERMISSIBLE PREVENTIVE ACTIVITIES

**6.** In Part III, Chapter 7 and again at the beginning of this chapter we took the position that the essential function of the security intelligence agency

[1] Criminal Code of Canada, section 2.

should be to collect, analyze and report intelligence and that the agency's mandate should not include certain types of countering and should exclude any executive powers for enforcing security. Here we will survey the various preventive or countering activities in which the R.C.M.P. Security Service has participated in the past and which might conceivably be envisaged for a security intelligence agency in the future, in order to set out more precisely which of these activities are permissible, which are dubious, and which are unacceptable. The principle of the rule of law which must apply to all security intelligence practices and policies requires a clear prohibition of any preventive or countering technique which violates any law — federal, provincial or municipal. The preventive techniques discussed below all relate to practices which are lawful.

*Reporting security intelligence to governments and police forces*

**7.** In the preceding chapter we reviewed the reporting functions of the security intelligence agency, pointing out the contexts in which components of the federal government and the R.C.M.P. require security intelligence in order to fulfill their responsibilities. In the next two chapters we shall consider the conditions under which the security intelligence agency should be authorized to transmit information to foreign governments and to provincial and municipal authorities in Canada. Such properly authorized transmission of security intelligence is not only a permissible way for the security agency to participate in preventing or countering threats to security but is indeed the overriding *raison d'être* for the existence of a security intelligence organization. But this reporting role, it must be emphasized, involves the transmission of information to public bodies — to police and government departments — under properly authorized law enforcement or security programmes.

*Preventive security interviews or briefings*

**8.** There are a number of contexts in which the security intelligence agency may wish to warn individuals and organizations in the private sector about threats to security. Canadian public servants or employees of private firms which have access to classified information who are about to be posted to missions in certain foreign countries, or civilians who are intending to travel in those countries, should be warned about the methods known to have been used by foreign intelligence agencies to compromise persons and through blackmail induce them to become sources for the foreign agency. We think this is an acceptable use of security intelligence and it is best for a member of the agency to give the briefing. However, such briefings should be given only to persons who are in a position to do serious damage to national security if they are compromised. Also, the agency should not use these briefings as a pretext for recruiting an individual to serve on a continuing basis as an intelligence source. In Chapter 4 of this Part we specified the conditions under which such continuing casual sources should be used as a means of collecting information. When those conditions are met and the agency is authorized to use a person who may travel abroad as a continuing source of information, it should not approach the individual in a surreptitious manner for that purpose. Openness

and voluntariness should be characteristics of the agency's security briefings of individual Canadians.

**9.** In the past, the Security Service has been known to communicate information to the employer of a person suspected of participating in, or supporting, a subversive activity, in order to jeopardize the employment of such persons (Vol. 41, p. 6709; Vol. 52, pp. 8426-7). We think that this practice is unacceptable. Denying a person employment in the public or private sector for national security reasons is a significant executive act which should be carried out only through authorized security clearance programmes. If the security intelligence agency has information indicating that a person in a firm which is carrying out defence-related work or work relating to national security is a security risk, it should pass that information to the department of the federal or provincial government responsible for the defence or security programme.

**10.** In at least one major Canadian city the Security Service undertook a programme of visiting senior officials in different sectors of community activity. One purpose of this programme was to make private employers aware of the availability of the Security Service in case they had reason to be concerned about subversive employees. We consider this a dangerous and unwise programme in that it is likely to lead to an exchange of information between private employers and the security intelligence agency which, again, may jeopardize the employment opportunities of individuals. Further, we do not think a security intelligence agency should advertise its services to the private sector. If the government deems it necessary to alert private organizations to the availability of the security intelligence agency to receive reports about threats to security, the government should do so through a vehicle other than the security intelligence agency.

**11.** We also think that the practice of giving security briefings to private groups to alert them to threats to security should not be permitted. Participation in activity of this kind may be perceived to be, or may in fact become, a propaganda campaign by the security intelligence agency. We think the dissemination of information about threats to security should be left to responsible Ministers. Mr. Justice Hope reached a similar conclusion with respect to the Australian Security Intelligence Organization:

> 248. It is no part of ASIO's intelligence dissemination function to publicize threats to security. Any D.G. of Security who reads s.5(1)(a) of the ASIO Act as authority to engage in propaganda, however 'laudable', embarks on a misconceived enterprise. The likely result is to bring discredit to ASIO.
>
> 249. A propaganda activity of this kind crosses the boundary between provision of information, which is proper, and the taking of a 'measure for security', which is not proper.
>
> 250. If warnings about the internal security situation are to be given publicity — whether attributably or not — that is something for the Government. It can seek advice from ASIO, or be offered it, and publish it. But the agency of publication should not be ASIO. Our system of government requires ministers to submit themselves to questioning in or out of Parliament. They have the responsibility and not ASIO.

> 253. If ASIO becomes involved directly in the public dissemination of security intelligence, it is likely to be accused of taking a partisan political position. It is most important that ASIO be above reproach in that regard. In many respects, its effectiveness depends on it having the confidence of all the major political parties.[2]

We agree with Mr. Justice Hope's reasoning. We would add that if the Director General or any other member of the security intelligence organization is to make a speech or otherwise appear in public to describe the work of the security agency or to give advice about threats to security, he must do so only with the permission of the Minister responsible for the agency, and only for the purpose of explaining or expounding government policy. In our view, for the reasons advanced by Mr. Justice Hope, the Minister would be well advised not to involve the Director General or other members of the agency in this kind of activity.

*Relations with the press*

**12.** For a number of years the Security Service carried on a press liaison programme, one purpose of which was to cultivate relationships with journalists that would enable the Security Service to "plant" certain material in the press. The articles were aimed at drawing attention to the security implications of certain events or the background or activities of certain individuals. (See, for example, Vol. 315, pp. 301427-63.) The cultivation of journalists was also designed to improve the Security Service's public image and to counter adverse publicity.

**13.** We think that the carrying out of a press liaison programme of this kind is seriously wrong. As we have said, it should not be a function of the security intelligence agency to publicize threats to security. If the agency requires any public defence of its activities or improvement of its image, this should be done by responsible Ministers. Secret intelligence agencies pose a serious threat to the democratic order when they endeavour to develop their own undercover media networks. That is why in our discussion of the use of human sources we recommended that the use of journalists as informants be very strictly controlled. We see no reason whatsoever for the security intelligence agency to maintain a press liaison programme or even a press liaison officer. Questions about the activities of the security intelligence agency should be answered by the Solicitor General or the Prime Minister. In Part VIII of this Report, we shall stress that one of the responsibilities of the Solicitor General, as the Minister responsible for the agency, is to provide opportunities for Members of Parliament and for the general public to study policy issues relating to the work of the security intelligence agency. It is important to provide a basis for a better public understanding of the function of the security intelligence agency, but this basis must not be established through a network of press relations established by the agency.

---

[2] Australia, *Fourth Report of the Royal Commission on Intelligence and Security*, Volume 1, pp.128-130.

*Disinformation and smear campaigns*

**14.** Attempts by a security intelligence agency to disrupt a domestic political group by circulating information about certain of its members constitute another category of unacceptable preventive activity. Such tactics, or "dirty tricks", are unacceptable even if they involve no breach of the civil or criminal law. The security intelligence agency should not be permitted to inflict damage on individual Canadians or Canadian organizations. In our liberal democratic system the state should administer sanctions against a citizen only when it has been established by due process of law that the citizen has broken the law. 'Disinformation' campaigns by the security organization run the risk of misleading not only the targetted group, but also other police forces and the government.

**15.** The prohibition of this type of disruptive activity should extend to the use of such tactics as anonymous letters or telephone calls designed to breed distrust amongst members or between factions of domestic political groups. It should not be a function of a security intelligence agency to break up Canadian political organizations, even those suspected of supporting or participating in activities constituting threats to the security of Canada, by trying to manipulate their affairs secretly. The collection of intelligence about such groups by the agency may well enable those who are responsible for law enforcement or other executive programmes to take action against such groups. The process of collecting intelligence, especially through informants and defectors from such groups, may well have disrupting effects. But spreading information deliberately in order to disrupt such groups should not be permitted.

*Disruptive measures which mislead other government officials*

**16.** In one case which was part of Operation Checkmate, Security Service officials did not raise security objections about a certain individual who was applying for Canadian citizenship. They reasoned that doubts might be raised among this person's colleagues, should he suddenly be granted citizenship after a number of prior refusals. There is no evidence to suggest that the Security Service officials informed either their own Minister, the Minister responsible for the Citizenship programme or the Interdepartmental Committee on Citizenship, the body of officials responsible for reviewing citizenship applications, about this operation.

**17.** It is our opinion that deceiving other government officials in this matter is unacceptable behaviour on the part of a security intelligence agency. Should the agency in future wish to use another government programme to help deceive one of the agency's subjects of surveillance, then the Minister responsible for the agency should inform the Minister responsible for the government programme in question and seek his concurrence or seek to have the other department take the required action.

*Disruptive effects of double agents and informants*

**18.** The use of informants by the security intelligence agency is very likely to have direct disruptive effects on penetrated groups or organizations. In the

counter-espionage field this is certainly the case with double agent operations, where an attempt is made to recruit a member of a hostile foreign service to be a source of information about the intentions and resources of the foreign agency and to influence the decisions of the foreign agency in a direction Canada would prefer.[3] Such operations, if successful, may enable the security agency to inflict serious damage on the foreign agency. The application of such methods in the counter-intelligence field against agencies of hostile foreign powers is an acceptable, indeed a highly desirable, preventive activity for the security intelligence agency, providing it is carried out in Canada. Similarly, the agency should be authorized and prepared to assist members of hostile foreign agencies who wish to defect while in Canada.

**19.** Informants may also be used by the security intelligence agency to gather information about a domestic political organization where there is reason to believe it is planning serious political violence. The presence of informants in such organizations may certainly have disruptive effects, but so long as the informant's primary purpose is to provide the security intelligence organization with information this is an acceptable activity. It becomes unacceptable when it is primarily a scheme of political interference designed to break up the organization. A cynic might say that in practice this will become a meaningless distinction: in our view it is a distinction which can be maintained, provided the members of the security intelligence agency understand and accept the reason for it. On the other hand, it will not likely be maintained if members of the agency, especially its senior officers, fail to appreciate that active intervention in the political process by a secret state agency endangers Canadian democracy.

**20.** Having said that an informant must not be injected into a domestic political organization for the primary purpose of disrupting the organization, even though it is planning political violence *generally*, we think that an informant who has penetrated a political organization for intelligence gathering purposes should be instructed that, when persons in the organization form an intent to commit a *specific* crime, the informant should try to discourage and inhibit the members of the organization from carrying out that crime. We note that such an instruction is included in the guidelines governing the F.B.I. use of informants, issued by the Attorney General, Mr. Levi, in 1976.[4] But we also note that in his testimony to a Congressional Committee, Mr. Levi stated that such disruptive actions must be "the minimum necessary to obstruct the force and violence" and "designed and conducted so as not to limit the full exercise of rights protected by the Constitution and laws of the United States."[5]

---

[3] For a good account of this counter-intelligence strategy in wartime, see John Masterman, *The Double Cross System*, New York, Avon Books, 1972.

[4] Attorney General's Guidelines for F.B.I. Use of Informants in Domestic Security, Organized Crime, and other Criminal Investigations, December 15, 1976. Quoted in John T. Elliff, *The Reform of FBI Intelligence Operations*, Princeton, New Jersey, Princeton University Press, 1979, Appendix IV.

[5] Quoted in John T. Elliff, *The Reform of FBI Intelligence Operations*, Princeton, New Jersey, Princeton University Press, 1979, p. 129.

**21.** In using the words "to discourage and inhibit" we wish to make it clear that in no way do we understand them to mean that the informant is licensed to break the law in order to achieve his specific objective of discouraging or inhibiting the crime. We envisage that there are ways of discouraging or inhibiting the commission of a specific crime which do not in any way entail the transgression of the law. To that extent we are in agreement with the Guidelines issued by Mr. Levi in 1976. Section 27 of the Criminal Code is a clear illustration of the latitude which may be exercised under the law. That section reads:

> Everyone is justified in using as much force as is reasonably necessary
>
> (a) to prevent the commission of an offence
>
> (i) for which, if it were committed, the person who committed it might be arrested without warrant, and
>
> (ii) that would be likely to cause immediate and serious injury to the person or property of anyone or
>
> (b) to prevent anything being done that, on reasonable and probable grounds he believes would, if it were done, be an offence mentioned in paragraph (a).

*Defusing*

**22.** 'Defusing' is a technique designed to reduce the possibility of violence by groups. It is accomplished by having members of the security intelligence agency speak to members of the group, letting it be known that the agency is aware of the group's plans to use violence. The expectation is that this will cause the group to have second thoughts. Also the agency might point out acceptable non-violent ways in which the group can pursue its political objectives. Such defusing programmes or 'constructive encounters' have been said to be analogous to the English policeman's gentle and good natured admonition to members of a restless crowd to "move along, there". We consider that a word of caution and encouragement to use non-violent means of publicizing a group's cause are perfectly proper techniques of preventing disorder in a democratic society. However, we are not convinced that such defusing actions should be a responsibility of Canada's security intelligence agency.

**23.** Under the statutory mandate which we have recommended for the agency, much of what might be referred to as civil disorder would not be within the purview of the security intelligence agency. The resort to violence by political groups should be of interest to the security intelligence agency only when it constitutes terrorism or a serious threat to the democratic order. But even where the threat of political violence is within the intelligence collection mandate of the agency, we do not think it is the most appropriate body to attempt defusing actions. It would be preferable for police forces, with local peace officer responsibilities, to employ such techniques. There is also a practical consideration: using members of the agency in such a programme decreases their availability for covert operations by revealing their identity as members of the agency to too many people.

*Conspicuous surveillance*

**24.** 'Conspicuous surveillance' is a technique of intimidation whereby members of a security intelligence agency, by making a group aware of their presence, attempt to frighten the group into abandoning its meeting or demonstration. To equate such conspicuous surveillance by members of a security intelligence agency with the presence of uniformed police officers at a public meeting or demonstration at which violence may break out is to use a false analogy: the presence of policemen in those circumstances is a legitimate means of dampening the possibility of immediate violence. They are identifiable as police and there is nothing in their deployment that smacks of intimidation by the state for a purpose other than law enforcement. It is not acceptable to use security intelligence officers in civilian clothes, in large or small numbers, to intimidate Canadians attending political meetings, even meetings at which the intention to use political violence is promulgated.

**25.** The common theme in our approach to the techniques of countering or preventing threats to security is that the security intelligence agency should not be permitted to carry out activities or disruptive measures designed to inflict damage on Canadian citizens or domestic political groups. The agency should concentrate on the collection and analysis of intelligence, the 'countering' of foreign intelligence agency operations in Canada, and the transmittal of intelligence to the appropriate departments of government so that *they* may take whatever action *they* deem to be in the public interest. A distinction should be drawn between the extent to which 'countermeasures' are taken against spies and international terrorists on the one hand, and against domestic subversive groups on the other. In the former cases, it is permissible to 'weaken' the adversary by recruiting an agent in place who will attempt to shape the decisions of the hostile agency or group, or by encouraging a hostile agent to defect. But in purely domestic matters, the purpose of penetration should be solely the collection of intelligence rather than disruption. Of course, if the target is a Canadian citizen acting as a foreign agent these activities are not a purely domestic matter, but even in this case we consider it undesirable for the agency to engage in any disruptive activity if the Canadian is an active member of a recognized Canadian political party. In domestic matters, if there is evidence of the commission of a crime, the security intelligence agency may turn it over to the police having jurisdiction in criminal matters, a perfectly acceptable kind of countering in all situations.

**26.** We do not recommend any system of prior approval of countering measures, because we do not envisage the use of any countering measures which are not part of authorized and acceptable intelligence collection methods. Some might regard the position we have taken against countering programmes by a security intelligence agency as unreasonably severe. However, we believe that this position is justified on the basis of the damage which the employment of such techniques, even when lawful, may do to the democratic process and to the security intelligence agency itself. Nothing has done more to discredit secret intelligence agencies in the western democracies, including Canada, than their perpetration of 'dirty tricks' on the citizens of their own country. The securing of democracy requires an effective security intelligence

agency. That effectiveness requires that the agency have broad public support. That support must not be alienated by unacceptable countering or disruptive activities.

**WE RECOMMEND THAT the security intelligence agency not engage in making known to employers in the private sector its availability to receive information about employees alleged to be subversives, and that any such advice as to such availability should, if the government considers such advice to be desirable, be transmitted through another department or agency.**

(35)

**WE RECOMMEND THAT it not be a function of the security intelligence agency to publicize, outside government, threats to the security of Canada; and accordingly, the security intelligence agency should not maintain liaison with the news media; and further, that all public disclosure about the activities of the security intelligence agency should be made by responsible Ministers.**

(36)

**WE RECOMMEND THAT the security intelligence agency not be permitted to disseminate information or misinformation in order to disrupt or otherwise inflict damage on Canadian citizens or domestic political organizations.**

(37)

**WE RECOMMEND THAT if the security intelligence agency wishes to use another government programme to help deceive one of the agency's subjects of surveillance, the Solicitor General should seek the concurrence of the Minister responsible for the programme in question.**

(38)

**WE RECOMMEND THAT the security intelligence agency not be permitted to use informants against domestic political organizations primarily for the purpose of disrupting such organizations.**

(39)

**WE RECOMMEND THAT an informant of the security intelligence agency who has penetrated a political organization for intelligence gathering purposes should be instructed that, when persons in the organization have formed an intent to commit a *specific* crime, the informant should try to discourage and inhibit the members of the organization from carrying out that crime, but that the informant must not transgress the law in order to discourage or inhibit the commission of the crime.**

(40)

**WE RECOMMEND THAT it not be a function of the security intelligence agency to carry out defusing programmes and that the agency not be permitted to use conspicuous surveillance groups for the purpose of intimidating political groups.**

(41)

## C. INTERROGATION OF SUSPECTS

**27.** In Part III, Chapter 10, we pointed out that there may be interrogations of persons within the Security Service suspected of having become agents for a

foreign intelligence agency. Here we wish to stress the importance of observing the law in conducting such interrogations. So long as the Security Service is within the R.C.M.P., the provisions of the R.C.M.P. Act and Regulations as to the questioning of regular members must be adhered to. Civilian members are not subject to the same rules. If a civilian member is suspected, he must not be detained for questioning unless the police are prepared to arrest him for an offence. Of course, if a civilian member does not co-operate willingly, he will certainly prejudice his employment.

**28.** If a member of the security intelligence agency or an employee of another federal government department is questioned (for example an employee of the Department of External Affairs who has returned from a foreign posting) the members of the security intelligence agency must remember that there is in our law no general power to detain for questioning.[6]

**29.** If, as we recommend, the functions of the Security Service are in the future exercised by a security intelligence agency separate from the R.C.M.P. and without police powers, it will be particularly important to ensure that the members of the agency are conscious that, just as the police have no power to detain anyone against his will for questioning, so too no civilian person has such a power.

[6] Leigh, *Police Powers in England and Wales*, London, Butterworth's, 1974, p. 29.

# CHAPTER 7

# INTERNATIONAL DIMENSIONS

## INTRODUCTION

**1.** The origins of many of the threats to Canada's internal security are located outside of Canada. Clearly, the security intelligence agency whose function it is to provide advance intelligence about threats to Canada's security should be able to obtain information about the foreign sources of these threats.

**2.** There is a considerable body of public information about international trends and events which the security intelligence agency can and should use. For instance, the branch that deals with Communist bloc intelligence activities and the branch that deals with Marxist and Leninist organizations in Canada should have a capacity for analyzing publications describing the international policies of Communist countries and international trends in Marxist and Leninist political movements. The security intelligence agency should also have effective liaison with the Department of External Affairs so that it can make good use of the understanding of international trends acquired by Canadian missions abroad.

**3.** However, because of the highly secretive character of foreign security and intelligence agencies and international terrorism, much information about activities directed against Canada's security from abroad cannot be obtained through public sources of information. Canada, unlike most of its allies, has not developed a foreign intelligence service. When we speak of a foreign intelligence service we mean an agency which collects abroad, by overt and covert means, intelligence on security, economic, political and military matters relating to other countries, which may be of interest to Canada. On occasion, and more in the distant past than in recent years, Canada has used secret agents abroad to collect information pertinent to Canada's internal security. But for the most part Canada has relied on its allies for foreign intelligence about threats to the country's security.

**4.** There is some information that friendly foreign agencies will not collect, if only because they have no need to or no interest in doing so if their national interests would not be served. Some of this information may be obtained through extensions abroad of security intelligence investigations initiated in Canada. In this way an extra-territorial dimension is added to the activities of the Canadian Security Service. In section A of this chapter, we explore the circumstances in which we think it appropriate for members or agents of the security intelligence agency to go abroad for operational purposes.

**5.** Information provided by the intelligence agencies of a large number of countries has been an important source of security intelligence for Canada in the past. It has not been forthcoming without a willingness on the part of Canada's Security Service to exchange information. In section B of this chapter, we will look at some of the current problems involved in the exchange of information with foreign agencies. We will suggest that guidelines be drawn up to govern such relationships generally, and that terms of reference governing particular relationships with foreign agencies conform to these guidelines. We also suggest the kinds of information which should and should not be exchanged, and outline a system of controls for monitoring relationships.

**6.** In section C we turn to a more speculative question: whether or not Canada should establish its own secret foreign intelligence agency. We make no recommendations on this subject, but urge that it be carefully studied. To look at this question following our consideration of the foreign activities of the Canadian security intelligence agency and its relations with foreign agencies is, we think, appropriate, since part of the difficulty in defining the proper circumstances for members of the security intelligence agency to go abroad arises from Canada's lack of a foreign intelligence service. As regards relations with foreign agencies, this country is in a position of considerable dependence on its allies for information necessary for the identification of security threats to Canada.

## A. FOREIGN OPERATIONS UNDERTAKEN BY THE SECURITY INTELLIGENCE AGENCY

**7.** What, if any, operations should the security intelligence agency conduct outside Canada? Currently this issue, as it affects the R.C.M.P. Security Service, is clouded by a lack of clear guidelines within that agency, together with a lack of clear policy within government. This is compounded by confusion as to what constitutes 'defensive' and 'offensive' activities. Consideration of overseas operations carried out by the security intelligence agency is made more difficult, in the Canadian context, by the fact that Canada does not deploy a foreign intelligence service engaging in espionage in and against foreign countries. The difficulty arises from the resulting notion that the Canadian Security Service has not operated secretly abroad. It has, from time to time. While Canadians have not conducted espionage abroad, they have collected information secretly. This has created sensitivity both inside and outside government concerning Canadian security intelligence activities carried out in foreign countries.

**8.** Questions concerning a security intelligence agency's operations abroad are closely related to questions concerning the agency's relationships with "friendly" foreign agencies. If Canada wishes to obtain intelligence about activities in other countries which threaten the security of Canada, intelligence not openly available, Canada must either collect the information covertly or obtain it from an intelligence agency of a friendly country. To the extent that Canada chooses not to collect such information itself it must depend on obtaining this informa-

tion from friendly agencies. We will examine these arrangements in section B of this chapter.

*Historical background*

**9.** The historical section of our Report (Part II, Chapter 2) showed that there was a time in Canadian history when security intelligence was collected on a systematic basis, at least in the United States. This was particularly true of the period between 1864 and 1871 when Sir John A. Macdonald personally directed Gilbert McMicken's Western Constabulary to infiltrate Fenian groups in the United States. Thereafter, foreign intelligence operations became more spasmodic. At the turn of the century, rumours of American plots to annex the Yukon were investigated through the surveillance of suspected plotters in the United States and Canada, and through the infiltration of some American miners' organizations. The first World War saw further activities in the United States, directed principally from British Columbia, against agents suspected of espionage and subversion. The information from these operations was sent to Ottawa and to British authorities. Before the United States' entry into World War I the Commissioner of the R.N.W.M.P. directed, from the Force's Headquarters in Regina, investigations of persons of German and Austrian extraction suspected of launching espionage or sabotage activities against Canada from the western United States.

**10.** Since the formation of the R.C.M.P. in 1920, there has been no systematic collection overseas of security intelligence information by the Force. We have no evidence that this practice arose from a decision of government. Apparently it was a decision reached within the R.C.M.P. The policy did not, in itself, imply there was no need for Canada to collect information overseas. It simply meant that Canadians would not be deployed abroad to collect secretly such information.

*The proper scope of security intelligence activities outside Canada*

**11.** In the past, policy discussions of the Security Service's foreign operations have frequently focussed on the distinction between an 'offensive' and a 'defensive' intelligence agency. It has been argued that, because the Security Service is strictly a 'defensive' service, it should not operate abroad. According to this argument foreign operations should only be carried out by an 'offensive' agency. We do not find this distinction between an 'offensive' and 'defensive' agency helpful, since the distinction could refer to three different aspects of intelligence operations:

(i) the kind of intelligence which an agency seeks

(ii) whether the collecting agency attacks foreign agencies which are targetted against Canada or waits to defend itself against foreign attacks

(iii) the geographic location of the agency's activities.

Discussions of 'offensive' and 'defensive' intelligence agencies often fail to make clear which of these three aspects is being referred to. Failure to

distinguish amongst them may lead to great confusion in defining the proper scope of the foreign operations of a security intelligence agency.

**12.** First, so far as the nature of intelligence being sought is concerned, the mandate we have recommended for the security intelligence agency might be termed 'defensive' in the sense that the intelligence it seeks must pertain to threats to Canadian security. Its intelligence mandate should be confined to activities against the security of Canada generated by others — individuals, groups or countries. In this sense the security intelligence agency is a *counter-intelligence agency*, not an espionage agency.

**13.** Turning to the second dimension of a security intelligence agency — whether it attacks or simply defends — it is also clear from what we have recommended with regard to the use of countering activities (e.g. double agent operations in the counter-espionage field) that the security intelligence agency should not be entirely confined to a defensive posture. In Canada, but not abroad, it should be able to attack foreign agencies by penetrating them and gaining defectors; it should not be required to wait until it, or some other branch of Canadian government, is being attacked. To borrow from the language of sports, the best defence is sometimes a good offence.

**14.** Now, turning to the third dimension — the geographic location of the security intelligence agency's activities — we do not think that the agency should be required to confine its intelligence collecting or countering activities to Canadian soil. If security intelligence investigations which begin in Canada must cease at the Canadian border, information and sources of information important to Canadian security will be lost. Thus a total ban on security intelligence operations outside Canada would be an unreasonable constraint. If to operate abroad is 'offensive', then Canada's security intelligence agency should be offensive in this sense, although we are cognizant of the very great risks — diplomatic, moral and practical — in carrying out security intelligence activities abroad. Because of these risks it is important to confine such activities to those that are essential, to subject them to a clear and effective system of control, and to ensure that they are always within the mandate of the security intelligence agency. In what follows we shall endeavour to define more precisely the circumstances in which a security intelligence agency should be permitted to extend its operations abroad and the controls which should apply to such operations.

*Current practice*

**15.** Covert Security Service operations outside Canada today are conducted on an *ad hoc* basis. These cases involving foreign travel always arise from an internal security investigation begun in Canada. Generally, the rationale for such operations is that the information sought relates directly to the internal security of Canada and is not the kind of information that can be or should be obtained through liaison with friendly security and intelligence agencies.

**16.** It is important that the distinction be made between occasional travel abroad by members of the R.C.M.P. Security Service for operational purposes, and the activities of R.C.M.P. liaison officers posted to Canadian missions

abroad. The 48 liaison officers stationed in 26 posts abroad perform two functions for the Security Service: they screen immigrants applying for entry to Canada in order to establish which individuals have criminal records or are suspect from a security point of view, and they carry out liaison with the police and security agencies of the host country. The liaison officer's functions do not include the direction of cases involving the collection of intelligence by covert means.

**17.** Many nations deploy both a security intelligence agency and a foreign intelligence service. Canada is unique among its close allies in that it does not have a secret foreign intelligence service. This country's non-involvement in covert foreign operations, or espionage, was most recently stated by Prime Minister Trudeau, when he told the House of Commons that:

> We have never, to my knowledge, certainly not under my government, engaged in any espionage abroad in the sense that we have not been looking for information in an undercover way in any other country.[1]

**18.** To clarify the circumstances under which foreign operations might be permitted, we felt it might be helpful to review past operations. The cases we reviewed could be divided into three categories which correspond to low, medium, and high levels of risk in foreign operations: the element of risk pertains not only to the individuals concerned, but to Canada's relations with the state against whom the operation is mounted, or the state in which it takes place. In the course of this work we identified some areas where a high risk was evident. If Canada is to mount foreign operations in the future, it is our view that it is inappropriate for a Canadian security intelligence agency to carry out some particular types of high risk operations.

**19.** Decisions as to when a foreign operation by the security agency should be permitted must be guided by a balancing of costs and benefits. Without attempting to be exhaustive, we would suggest that at least the following considerations be taken into account:

(a) the intelligence 'target' of the foreign operation must be one which is within the security intelligence agency's mandate;

(b) a foreign operation involving clandestine activity should be undertaken only for the purpose of obtaining information which is of great importance to the security of Canada, or for maintaining an intelligence asset which is of great importance to the security of Canada;

(c) wherever possible the security intelligence agency should work co-operatively with the security agency of the host country; the cumulative effect of unilateral Canadian operations abroad might invite retaliatory actions which could be detrimental to Canada's security and foreign relations;

(d) transgressions of foreign laws would not be taken as having been authorized by the mere fact of authorization having been granted for travel to a foreign country, and the agency should place the problem before the Cabinet for a decision as to what should be permitted;

---

[1] House of Commons, *Debates*, January 10, 1974, p. 9227.

(e) the Minister responsible for the security intelligence agency and the Minister of External Affairs should be kept adequately informed of security intelligence operations outside of Canada.

We turn now to the controls which should regulate foreign operations of a security intelligence agency.

*Controls*

**20.** Under the present system there are certain stages through which a foreign operation must go for approval before the operation occurs. We examined these stages, and it is significant that within these reporting relationships, as now prescribed, there is no provision for notifying the Solicitor General, the Minister responsible for the Security Service.

**21.** So far as control within the security intelligence agency is concerned, we think the Director General should be notified of all foreign operations. As the chief executive officer of the security intelligence agency, he should have the opportunity to question any foreign operations and to veto those which he thinks are inadvisable. There may be emergency circumstances in which the Director General is not immediately available, in which case he should name his deputy on a *pro tem* basis, as responsible for giving his approval for any such operation.

**22.** At the ministerial level we think that it is intolerable to continue with a situation in which the Minister responsible for the security intelligence agency is not informed of foreign operations. The Director General should notify the Solicitor General before initiating any foreign activity involving a member of the agency or its informants. The Minister's review of such proposals should be based on a set of policy guidelines, prescribed by him, governing foreign operations. These guidelines would incorporate the factors suggested in paragraph 24 above. These guidelines should also be approved by the Cabinet Committee on Security and Intelligence and disclosed to the special Parliamentary Committee on Security and Intelligence. It is important that guidelines in this area be subject to a collegial interdepartmental approval process, as they should reflect the various concerns of government that must be balanced in determining the advisability of foreign operations by an intelligence agency. The statute governing the activities of the agency should include authorization to operate abroad.

**23.** We recognize the need to ensure that foreign operations by a security intelligence agency are co-ordinated with the requirements of Canada's foreign relations. Even though we anticipate that the number of foreign operations undertaken by the security intelligence agency will be low, still certain of these operations might, if improperly handled, cause grave damage to Canada's international relations or run counter to Canada's foreign policy objectives. We do not think, however, that all foreign operations by a security intelligence agency incur such risks. Some of the cases we reviewed involve low-level risks. Moreover, in our view, it would be desirable that in any foreign operations contemplated in the future, the following two practices be followed:

(1) The Minister responsible for the security intelligence agency should notify the Department of External Affairs in advance of any operations entailing significant risks to Canada's foreign relations. In an emergency situation, a foreign operation could go ahead with the provision that notification took place *ex post facto.*

(2) On an annual basis, the Director General and appropriate officials of the security intelligence agency should meet with the Under Secretary of State for External Affairs and the Deputy Under Secretary of State for Security and Intelligence to review foreign operations completed, currently being undertaken, or proposed by the security intelligence agency.

The system we propose recognizes that it is a ministerial responsibility to ensure that the Department of External Affairs is consulted in advance about foreign operations with serious implications for foreign policy and provides a process whereby the Department of External Affairs can be kept comprehensively informed of the security intelligence agency's foreign operations.

**24.** There may well be situations in which the Department of External Affairs would consider that the risk to Canada's foreign relations exceeds the potential worth of the security intelligence that might be obtained from a foreign operation. In resolving differences of this kind it is important that one set of interests should not automatically take precedence. Thus, when the Solicitor General and the Secretary of State for External Affairs could not agree over a foreign operation, the matter should be decided by the Prime Minister.

**WE RECOMMEND THAT for intelligence purposes falling within the security intelligence agency's statutory mandate and subject to guidelines approved by the Cabinet Committee on Security and Intelligence, the security intelligence agency be permitted to carry out certain investigative activities abroad.**

(42)

**WE RECOMMEND THAT the Director General of the security intelligence agency inform the Minister responsible for the agency in advance of all foreign operations planned by the security intelligence agency.**

(43)

**WE RECOMMEND THAT in cases which on the basis of policy guidelines are deemed to involve a significant risk to Canada's foreign relations, the Minister responsible for the security intelligence agency inform the Department of External Affairs sufficiently in advance of the operation to ensure that consultation may take place.**

(44)

**WE RECOMMEND THAT the Director General and appropriate officials of the security intelligence agency should meet with the Under Secretary of State for External Affairs and the responsible Deputy Under Secretary on an annual basis to review foreign operations currently being undertaken or proposed by the security intelligence agency.**

(45)

## B. RELATIONSHIPS WITH FOREIGN AGENCIES

**25.** One of Canada's major sources of intelligence about security threats to this country comes from foreign security and intelligence agencies. The largest suppliers of such information are agencies of countries with which Canada is closely allied. Even if this country had its own secret intelligence service working abroad, there would still be a need for agreements with foreign agencies.

**26.** Relationships with foreign security and intelligence agencies inevitably involve a sharing or exchange of intelligence: in order to receive information, Canada must be willing to give information to those agencies. The notion of reciprocity is, then, central to successful liaison relationships with foreign agencies.

**27.** Liaison with foreign agencies raises a number of important policy concerns. One is, simply, whether true reciprocity exists. There is always a danger that, unless the exchange of information is carefully monitored, Canada may give far more than it gets. A second concern relates to the entering into agreements which may conflict with Canada's foreign policies. An agreement should not be made with the agency of a foreign country if it would entail implicitly condoning policies which Canada has opposed as a matter of our foreign policy. A third issue involves the need for sufficient control over information leaving this country to ensure that the rights of Canadians are adequately protected.

**28.** These and other issues all point to the need for careful and accountable control by government of liaison agreements between the Canadian security intelligence agency and foreign agencies. From our review of this subject, it is evident that there has been a lack of government attention to the policy issues inherent in such agreements, a neglect which can create an excessive vulnerability to the hazards of liaison with foreign agencies.

**29.** Another, less tangible, problem related to foreign agreements is the danger of Canada's security intelligence agency adopting the outlook and opinions of a foreign agency, especially of an agency which has come to be depended upon heavily. This danger is particularly acute because Canada does not have its own foreign intelligence agency, so that a Canadian Security Service may become extremely dependent on foreign agencies for covert information. This tendency to adopt the views and analyses of a foreign agency would be offset if the security intelligence agency had at its disposal expertise capable of providing analyses derived from open literature. The R.C.M.P. Security Service has had few members capable of providing analyses of foreign situations with possible effects on Canadian security.

**30.** Some central issues have to be addressed regarding the identity and nature of the partners with whom the government is willing to enter into relationships, the extent of agreements including the kinds of information to be exchanged, and the procedures to be established to ensure that the agreements or relationships reflect both the wishes and the needs of the Canadian

government while balancing security interests with foreign policy interests. In what follows, we will set out our recommendations on these matters.

*Agreements with foreign agencies*

**31.** Relationships with foreign agencies are covered by a variety of agreements, both formal and informal, enduring and occasional, covering the exchange of different kinds of information and services. The R.C.M.P. currently has relationships with foreign agencies providing for many types of exchange, including information regarding terrorism, visa vetting of immigrants, information given to foreign agencies on Canadian emigrants, and information regarding counter-espionage. This list is not exhaustive, but it gives some idea of the variety of relationships entered into by the R.C.M.P. Security Service.

**32.** One characteristic of the development of these relationships has been their *ad hoc* nature. They have been entered into as a result of a perceived need within the R.C.M.P. and have not been subject to an over-arching set of government guidelines. A more fundamental objection to the development of these previous agreements is that the Solicitor General, the Minister responsible for the R.C.M.P., has not been adequately informed about them until very recently. In 1977, the then Solicitor General, Mr. Fox, asked the R.C.M.P. to provide him with a list of all existing foreign liaison arrangements. To attempt to comply with the wishes of the Minister, the Security Service had to solicit information from its operational branches: no central record existed. It was only after much research by us and by the R.C.M.P. that by 1980 it had been determined that there were, in fact, arrangements with a great many countries. We mention this to emphasize the absence of any recording or control of such an important network of arrangements. As a result, the R.C.M.P. has proceeded independently to develop foreign agency arrangements in an area of foreign policy concern.

**33.** This is not to suggest that relationships with foreign agencies have been of a *sub rosa* nature. We simply make the point that two obvious points of control, the Department of the Solicitor General and the Department of External Affairs, have remained largely in ignorance of the existence or terms of such relationships. While we appreciate the sensitivity of information exchanges and the consequent need to limit knowledge of their existence within the government, we feel it particularly unsatisfactory that the Solicitor General, the Minister responsible for the Security Service, has not been consulted, nor his agreement sought, in the establishment of relationships with foreign security and intelligence agencies.

**34.** We think that the statutory mandate of the security intelligence agency should explicitly provide that there may be foreign liaison agreements subject to proper control. The principal points of control should be the two Ministers, the Solicitor General and the Secretary of State for External Affairs. No agreement should be entered into without terms of reference approved by the two Ministers. The terms of reference for each agreement with a foreign agency should specify what types of information or service could be exchanged

(for example, immigration visa vetting, and intelligence on terrorists). These terms of reference, while recorded within the Canadian government, need not necessarily be written down or formally agreed upon with the foreign agency. Some foreign agencies would withhold their cooperation if the Canadian security intelligence agency insisted on formal written agreements.

**35.** If agreement on terms of reference cannot be reached between the Secretary of State for External Affairs and the Solicitor General, the decision would be made by the Prime Minister. We would anticipate that any such disagreement would arise from competing considerations relating to foreign policy and security. It is important that one Minister not have the power of veto over a particular set of terms of reference, and that disagreements be resolved by the Prime Minister or the Cabinet.

**WE RECOMMEND THAT the statutory mandate of the security intelligence agency provide for foreign liaison relationships subject to proper control.**

(46)

**WE RECOMMEND THAT the terms of reference for each relationship specify the types of information or service to be exchanged.**

(47)

**WE RECOMMEND THAT the terms of reference for each relationship be approved by the Solicitor General and the Secretary of State for External Affairs before coming into effect and that any disagreement be resolved by the Prime Minister or the Cabinet.**

(48)

**36.** The government should establish a clear statement of principles to guide the security intelligence agency's relationships with foreign security and intelligence agencies. One purpose of these guidelines would be to diminish the risk of the security agency's becoming an appendage of foreign agencies, particularly in relation to those agencies from whom it borrows information frequently. These principles should be developed as a set of guidelines by an interdepartmental committee, and approved by Cabinet. In the following paragraphs, we suggest some of the principles that should be reflected in these guidelines.

*Exchanges of information with foreign agencies*

**37.** As we have indicated, an effective Canadian security intelligence agency requires information and intelligence from foreign agencies to meet Canadian needs. These foreign agencies may provide not only useful general assessments of potentially or actually dangerous situations, but also intelligence concerning individuals who may come to Canada or who are already here. Given the reciprocal nature of these relationships, the Canadian security agency must be willing to provide similar kinds of information in return.

**38.** With this understood, we are of the opinion that certain precautions have to be taken with regard to the information provided to foreign agencies by the Canadian security intelligence agency. In 1971, for example, Assistant Commissioner Parent sent letters to four foreign agencies enclosing the R.C.M.P.'s brief on the Extra-Parliamentary Opposition (E.P.O.) which included the

names of individuals in the Canadian Public Service believed to be involved to a greater or lesser degree in that movement, and the names of some individuals who were not even suspected of involvement. We have no objection to the provision of the general assessment of the situation to other agencies. Rather, our objections to this action are twofold: first, the evidence on which the E.P.O. list of names was based was not reliable and was therefore potentially misleading to a foreign agency as well as harmful to individual Canadians; and second, there was no knowledge of the use, if any, to which the information was to be put by the foreign agencies, nor any procedure for recovering the information once it had been used. There appears to have been, and there still appears to be, no consciousness on the part of the R.C.M.P. of these concerns in respect of that information. That, if symptomatic of a general attitude, is most disheartening and alarming.

**39.** The principle of reciprocity may also induce the Canadian security authorities, in their position of dependence, to enter into relationships with foreign agencies without giving adequate weight to possible conflicting foreign policy considerations. A lack of sensitivity in this area will, almost inevitably, create friction with those responsible for directing Canada's external relations.

**40.** A third facet of reciprocity is the assessment of the flow of information in and out of Canada. A relationship with a foreign agency which consistently results in a net outflow of information is clearly one which should be examined for its usefulness to this country. This is not to suggest that the R.C.M.P. Security Service's participation in the world intelligence community is not valued by its allies. It is important to Canada in terms of, for example, terrorism and foreign intelligence activities. Moreover, if Canada were unwilling to collect information and to exchange it with foreign agencies, there is the danger that those agencies would take steps to get it themselves in Canada, by developing agents and sources in this country. These real or potential problems, together with lesser ones not set out here would, we feel, be overcome by the precepts which follow.

**41.** There should be records of the transmittal by the security intelligence agency to foreign agencies of information concerning Canadian citizens, or persons in Canada, or Canadian organizations.

**42.** As well as recording the transmittal of information, the so-called 'third party rule' must apply to such information in order that some semblance of control be retained over Canadian proprietary rights to the information, although it is recognized that such 'control' may well be somewhat illusory. The third party rule stipulates that information given by one agency to another may not be passed on to a third agency or party without the approval of the original agency. This rule should govern further use of the information by the recipient, and would also facilitate its retrieval. The difficulty of retaining any real control over information sent to another agency is illustrated by the inability of the R.C.M.P. to recover information it had supplied for more than twenty years to a foreign agency. In June 1978, pursuant to a decision previously taken by Mr. Fox, Mr. Blais instructed the R.C.M.P. to cease providing such information and requested the return of information previously

provided. At the time of writing this Report the requested information has not been returned.

**43.** The information given to foreign agencies must be about activities which are within the statutory mandate of the Canadian security intelligence agency. Foreign agencies are likely to have different mandates and therefore are likely to ask for information about Canadians or about people in Canada which is beyond the Canadian agency's terms of reference. When this occurs, the Canadian security intelligency agency must refuse to go outside its mandate, even though this may result in a reciprocal loss of information for Canada. In Chapter 5 of this part of the Report, we set out our views on what information received from a foreign agency should be reported by the security intelligence agency. We said that, with few exceptions, the agency should report only information relevant to threats to the security of Canada as defined in its mandate.

**44.** We take the view, too, that the Canadian security intelligence agency, as a pre-condition for passing information to a foreign agency, should know the reason for the request. To provide information without questioning the request invites the danger that the security agency will operate according to the mandate of a foreign agency rather than according to its own terms of reference.

**45.** Management of liaison arrangements must take into account the importance to Canadian security of maintaining a relationship between the Canadian security agency and its foreign counterpart. In relationships where Canada is the net beneficiary in the flow of information, this will be a particularly important consideration. In exchanges involving information on international terrorism or counter-intelligence, there will likely be little conflict of interest. A more probable source of difficulty would seem to us to be in exchanges of information on domestic subversion, where Canada's standards may differ from those of the foreign agency seeking information, and where there may be insufficient concern for the protection of the interests of Canadian citizens.

**46.** Moreover in our opinion, it should be a fundamental principle that information disclosed by a potential immigrant within the immigration process is for the sole and exclusive use of the Canadian government, and should not be further disseminated or disclosed, unless there is a clear and important reason related to Canada's security and the approval of the Director General of the Canadian security intelligence agency has been obtained.

*The exchange of services and joint operations*

**47.** Cooperation with a foreign agency may also entail some joint operations with that agency. The cooperation may take the form of lending a human source to the foreign agency, borrowing a source from the foreign agency, or providing or receiving some other support. An instance in which the R.C.M.P. Security Service borrowed from a foreign agency was that of Warren Hart. The Security Service of the R.C.M.P. has also undertaken joint operations with friendly foreign agencies within Canada. We are satisfied that these operations have been approved by the Security Service as being justified in the Canadian

interest, and that every reasonable effort has been made to ensure that friendly foreign agencies not conduct operations on Canadian territory without the prior approval of the Security Service. As mentioned earlier, however, we are not satisfied with the extent to which the Minister has been informed of the occurrence of such operations.

**48.** We believe that all cases involving the exchange of sources must have the approval of the Director General of the security intelligence agency. Such cases must be within the mandate of that agency, hence relevant to Canadian security, and should, in addition, be carefully controlled by Canada. In cases where a foreign security agency requests assistance which falls outside the mandate of the Canadian security agency but concerns a criminal matter, the request should be passed on by the security intelligence agency to the relevant police force in Canada. In this way, the security agency would act as a central clearing house and recorder of requests from foreign intelligence agencies. Such a procedure would permit an effective review of such operations by the independent review body.

**49.** Elsewhere, we have reported on the use by the R.C.M.P. Security Service of journalists in the writing and publication of articles containing information believed by the Service to be true. If such a practice were to involve the R.C.M.P. in attempting to arrange Canadian publication of foreign information, that would be both dangerous and undesirable, because it could result in information being published in Canada which is both unreliable and inconsistent with Canadian interests. Toleration of such a practice would open the door to the possibility of foreign manipulation of Canadian public or official opinion. That would be unacceptable. As stated earlier in this Report, any publication of material at the instigation of the Security Service should require the approval of the Director General of the security agency and his Minister. This would apply both to articles of foreign origin and to those inspired by press contacts within the agency.

**50.** A final aspect of the exchange of services between foreign agencies and the Canadian security intelligence agency concerns security screening for immigration purposes on behalf of a foreign agency. Under our recommendations for screening in Part VII of this Report, the security intelligence agency would carry out few field investigations. It should have a tightly circumscribed mandate to collect information about character reliability for Canadian purposes and should not collect this information on behalf of a foreign agency. Foreign agencies must not be allowed to carry out their own field checks here. They must rely on interviewing individuals in their own country or at their consulate or embassy in Canada. In sum, only limited aid could be given to a foreign agency in this area, and that assistance would have to coincide with the Canadian screening programme. Any assistance beyond this would have to be negotiated on a government-to- government basis.

*Obtaining security intelligence outside liaison arrangements*

**51.** It may be necessary for the Canadian security intelligence agency to obtain information otherwise than through a liaison arrangement, from a foreign country whose law forbids the dissemination of information to foreign

governments. As we will point out in Part VII, Chapter 2, to authorize the Canadian security intelligence agency to establish a paid source, or otherwise to break the laws of a foreign country in order to obtain information about one of its citizens, would be imprudent. To us, a more attractive alternative would be bilateral discussions between the two governments to obtain the information. In most cases, interviews with potential immigrants will suffice.

**52.** The normal exchange of security intelligence may, with some countries, be prevented by a lack of cooperation between the Canadian security agency and the host agency. One solution is to rely on the assistance of the agencies of friendly countries who have members there, and who may be able to advise the Canadian authorities of security information relevant to a potential immigrant. This procedure carries with it some risk of exposure and subsequent embarrassment to the Canadian government. In such cases, risks must be weighed against potential benefits and the decision incorporated into the terms of reference drawn up for the relationship with the friendly agency.

*Statement of principles*

**53.** The foregoing discussion indicates a number of the principles which should be incorporated into guidelines governing the security intelligence agency's relationships with foreign agencies. Briefly, we would suggest that these guidelines include the following principles:

(a) all relationships should have approved terms of reference;

(b) all transmittal of information by the security agency should be recorded;

(c) the third party rule should operate so that the information transmitted to a foreign agency may be retrieved when it is no longer needed;

(d) the security agency should be aware of the reason for the request from the foreign agency and that reason must relate in some way to the security of the requesting country;

(e) all exchanges must be within the mandate of the security intelligence agency and hence relate to the security interests of Canada;

(f) Canada must control all foreign agency operations in Canada;

(g) the Director General of the security agency must approve of each joint operation; and

(h) the Minister responsible for the agency should be notified when a member of the agency goes abroad on behalf of the agency.

**WE RECOMMEND THAT the Government establish a clear set of policy principles to guide the security intelligence agency's relationships with foreign security and intelligence agencies and that the Joint Parliamentary Committee on Security and Intelligence be informed of these principles.**

(49)

**WE RECOMMEND THAT the information given to foreign agencies by the security intelligence agency must be about activities which are within the latter's statutory mandate; that the information given must be centrally**

**recorded; that the security intelligence agency know the reasons for the request; and that the information be retrievable.**

(50)

**WE RECOMMEND THAT the Director General approve of each joint operation with a foreign agency and ensure that Canada control all foreign agency operations in this country.**

(51)

**WE RECOMMEND THAT the Solicitor General be informed of each joint operation, or operation of a foreign agency, in Canada.**

(52)

*Liaison officers abroad*

**54.** The recommendations for change which we have presented here should not, in any substantial way, alter the current arrangements pertaining to R.C.M.P. liaison officers. Currently, all such liaison officers come under the R.C.M.P.'s Director of Foreign Services which is not part of the Security Service. We anticipate that, even with a separate security intelligence agency, it should be possible to substitute a member of that agency for a member of the R.C.M.P. in those posts that, at present, have more than one liaison officer. In those missions where now there is only one liaison officer from the R.C.M.P., it should be possible for a single liaison officer to supply information to both the R.C.M.P. and the security agency. As both organizations, under our proposals, would report to the same Minister, he should ensure that the liaison function involves no unnecessary duplication of services and that there is effective cooperation between the R.C.M.P. and the security agency.

**55.** The recruitment and training programme outlined elsewhere in this Report would, we feel, better prepare individuals for international postings. These individuals should have diplomatic status as has recently become the case with some R.C.M.P. liaison officers.

**56.** The relationship between the liaison officer and the Head of Post should remain as at present and as laid down within the terms of reference formulated for the Foreign Service of the R.C.M.P. These state that liaison officers will serve as an integral part of the mission, and will be responsible to the Head of Post. Despite the clear need for communication between these two individuals, we take the view that if the liaison officer wishes specially to safeguard some security intelligence by sending it to his headquarters without clearing it with the Head of Post, he should be able to do so. The receipt of such information should be recorded by the security agency headquarters so that, except in extraordinary circumstances, the Under-Secretary of State for External Affairs has access to it. Where extraordinary circumstances exist, the Director General should disclose them to the Solicitor General. The decision to widen access to this information would then rest with the appropriate Ministers and not with their representatives at a foreign mission.

**57.** The post-war period has seen western missions in the U.S.S.R. and eastern Europe under persistent and increasingly sophisticated technical surveillance by Soviet and Soviet bloc intelligence agencies. Throughout this period, a great deal of evidence has been collected by western security and

intelligence agencies about the use of microphones, radio transmitters, and other forms of eavesdropping and electronic interception equipment used against their missions. It is very often unknown what time lag there has been between the installation and its discovery. It has been, and continues to be a most serious problem. Historically, there has been disagreement within some departments and agencies of government as to the extent of the threat and, therefore, the resources that should be available to counter it. The departments and agencies of government should, through suitable intragovernmental arrangements, arrive at agreement on this type of threat and on the resources necessary to meet it.

**WE RECOMMEND THAT the security intelligence agency have liaison officers posted abroad at Canadian missions to perform security liaison functions now performed by R.C.M.P. liaison officers, except that in missions where the volume of police and security liaison work can be carried out by one person, either an R.C.M.P. or a security intelligence liaison officer carry out both kinds of liaison work.**

(53)

**WE RECOMMEND THAT the relationship between the liaison officer representing the security intelligence agency and the Head of Post be governed by the terms of reference as laid down for the Foreign Services of the R.C.M.P., but that the security intelligence agency's liaison officer have the right to communicate directly with his Headquarters and independently of the Head of Post when the intelligence to be transmitted is of great sensitivity. Except in extraordinary circumstances, which should in each case be reported by the Director General to the Solicitor General, such communications should be made available to the Under-Secretary of State for External Affairs.**

(54)

**WE RECOMMEND THAT the government examine, on a regular basis, both the resources which are being devoted to the technical security of Canadian missions abroad, and the policies and procedures which are being applied to the security of those missions.**

(55).

*Review of foreign liaison activities*

**58.** In addition to ministerial responsibility, we advocate three other points of reference for these activities. First, the security intelligence agency's annual report to Cabinet should include an account of the agency's foreign liaison activities. Second, the independent review body should ensure that the agency's relationships with foreign agencies fall within the statutory mandate and meet the guidelines set out by government. This review would be facilitated by the central recording of the terms of reference governing particular relationships. Third, the Joint Parliamentary Committee on Security and Intelligence should be informed of the principles governing such relationships and, where possible, should have access to the terms of reference of particular relationships. If a foreign agency objected to the terms of its relationship with Canada's security intelligence agency being disclosed to members of the Committee, then the Canadian government would have the choice of foregoing that relationship or of refusing the Committee's access to the terms of the relationship.

**WE RECOMMEND THAT the security intelligence agency's relationships with foreign agencies be subject to the following forms of review:**

**(a) An account of significant changes in these relationships be included in the security agency's annual report to the Cabinet;**

**(b) relations with foreign agencies be subject to continuing review by the independent review body;**

**(c) the Joint Parliamentary Committee on Security and Intelligence be informed of the principles governing the security agency's relations with foreign agencies and, to the extent possible, of the terms of reference of particular relationships.**

(56)

## C. SHOULD CANADA HAVE A FOREIGN INTELLIGENCE SERVICE?

**59.** Canada is unique among its major allies in not deploying a foreign intelligence service. While we are in no position to carry out a comprehensive review of Canada's foreign intelligence needs, a general look at the question of a secret foreign intelligence service is a natural outgrowth of our consideration of the policies and procedures governing a security intelligence service. We have already shown how the lack of a foreign intelligence agency limits the effectiveness of a security intelligence organization. In the previous section, we showed how Canada, through liaison arrangements with 'friendly' intelligence agencies, compensates, to some extent, for the lack of a foreign secret service of its own. Also we think it important to consider how the system of government control and accountability which we are recommending for a security intelligence agency should apply to a foreign intelligence service, if and when Canada decides to establish such a service.

*Previous studies of Canada's foreign intelligence needs*

**60.** There would have been little need for us to comment on this subject if previous studies of Canada's intelligence needs had examined the subject comprehensively, but those to which we have had access make virtually no mention of it.

**61.** The more recent general reviews of which we are aware are four in number.

**62.** Perhaps the most important of these studies was one carried out in 1970. Significantly, many of the points made regarding the lack of integration of intelligence with governmental decision-making are still valid one decade later. It noted the emphasis on military intelligence in Canada and the need for this country to follow the Americans and the British in a greater use of political and economic intelligence. The government was advised of the need for greater co-ordination of intelligence at the centre, via the intelligence committees, and to some extent this advice has been taken. A more general aim of the study, like others later, was to question, first, if Canada was getting its money's worth from certain areas of its intelligence program and secondly, if the collected intelligence was being used as efficiently as possible.

**63.** The various studies came to the conclusion that Canada was indeed getting its money's worth from its multilateral intelligence arrangements and allowed that the arrangements were, in fact, a bargain. The second question as to whether or not the best use was made of the intelligence, was directly or inferentially answered in the negative. The further study, carried out on economic intelligence, was set up specifically to look at the linkages between producers and consumers and methods of improving the use made of this intelligence within the consuming departments.

**64.** All of these studies pointed to two further, and potentially serious, shortcomings. The first was that the mechanisms for determining Canada's foreign intelligence priorities and requirements were inadequate. The second shortcoming was the lack of intelligence analysis either within departments or on an interdepartmental basis. Despite widespread agreement that the analytical capacity should be strengthened within the intelligence community, little would appear to have been done to bring it about.

**65.** The first shortcoming, the lack of definition of priorities and requirements, has to some extent been offset, at least so far as foreign intelligence is concerned, by the establishment of suitable intragovernmental arrangements. It should be remembered, however, that a definition of requirements and priorities depends in some measure on an analysis of current intelligence holdings and on identification of areas or subjects that require further intelligence collection. In short, an inadequate analytical capability will contribute to a lack of clarity in the definition of requirements and priorities. Where there is a need for detailed information, such as in tactical or current intelligence on particular issues, this vagueness in definition will impede the collection process. In matters of broad strategic intelligence, the lack of precision in defining requirements and priorities will be much less of an impediment to effective direction of the collectors.

**66.** Although the weakness of the intelligence analysis function was recognized in the past, it has not been remedied to date. A proposal we shall develop later in this Report, that the Intelligence Advisory Committee have a responsibility for writing current intelligence assessments and that a Bureau of Assessments be established to provide strategic assessments, would, we believe, be the basis for overcoming this shortcoming in Canada's intelligence system.

*The external environment and changing intelligence needs*

**67.** A nation's intelligence requirements depend on a variety of factors, such as its political, economic, and military aspirations, its geographic location, and its involvement in regional organizations. Meeting these requirements does not necessarily involve covert information only; in fact, most of the collection effort, at least in human terms, will probably be focussed on gathering overt information. The extent to which a nation collects covert foreign intelligence through its own resources will depend, among other things, on its financial resources, its ethics, its international posture and the extent to which it believes it can rely on its allies.

**68.** There has been a paucity of analysis of non-military intelligence requirements in Canada. The current multilateral arrangements were formulated and continue to function largely within the context of East-West relations and the military blocs which underpin those relations. These arrangements for sharing intelligence have been based on mutual aims and a common perception of threats. Political intelligence which is processed information on other nation's international political relations does not, generally, have this element of commonality; it entails a national, rather than collective, need. Similarly, economic intelligence, despite the interdependence of the leading economic powers, tends to be more national and less multinational in perspective. The emergence of non-military concerns as dominant foreign policy issues of western nations has altered intelligence requirements. The emergence of energy, for example, as a pre-eminent foreign policy issue, reduces the commonality of interests between advanced western nations.

**69.** This skewing of national intelligence needs, away from military intelligence and towards greater emphasis on economic intelligence, places Canada in a situation which is quite different from its earlier post-war experience. One result of the emergence of new issues and the changes in the international climate in the past decade, has been the blurring of the once clear distinction between one's friends and those whose friendship is less manifest or reliable. While these changes have not, from a military point of view, altered the alignment of forces and so given rise to novel military intelligence requirements, there is a demonstrably greater need for political and economic intelligence for national purposes.

*Factors to be considered in deciding whether Canada should establish a foreign intelligence service*

**70.** A first step in considering those intelligence requirements which are related to Canada's distinctive national interests is to identify those national needs that cannot be met through liaison arrangements with allies. There is likely to be a quite narrow set of intelligence requirements, of a political or economic nature, or related to Canada's domestic security, which is either of no interest or of a competitive rather than a collaborative interest to Canada's allies. However few in number, such requirements should be identified. The second step is to determine how the intelligence needed in these areas can be collected, if it is not available from overt sources. There are, generally, two means of collecting intelligence covertly. The first is technical collection. The second method is through human sources conducting espionage.

**71.** Human sources have the great advantage of being able to yield intelligence about human intentions — and it is frequently knowledge of intentions which is most valuable in defending a country's political and economic interests as well as warning it of foreign threats to its internal security. Another advantage is cost: human sources cost much less than technical sources, all the more so if only a small organization is envisaged with a capacity for collecting intelligence in only a limited number of places. While we are not in a position to put a price on establishing a secret intelligence service — the costs of its

equipment, training facilities, and professional support services, for example, we understand that the cost of operating a small service is modest.

**72.** The costs of *not* having a capacity for collecting foreign intelligence relevant to distinctive Canadian interests must be considered. The experience of some foreign countries suggests that the intelligence product of a modest secret service has been useful to these nations. How much more security and intelligence information would Canada receive from its allies if it contributed more to the common pool? While this cannot be answered firmly, it is not unreasonable to suppose that the amount of intelligence available to Canada would increase. Foreign experience indicates that information is available to a country's foreign intelligence agency through liaison with other agencies that does not flow either to its diplomats or to its domestic security service.

**73.** While it is possible to outline some of the benefits which might accrue to Canada by establishing a limited secret intelligence service, there are also some readily identifiable liabilities. To begin with, there is a clear political risk in a government directing espionage activities against other states. The image of honesty and straightforwardness in the conduct of international affairs may produce benefits to this country, particularly within a Commonwealth setting, that cannot be readily measured. What potential penalties might be incurred in acknowledging the existence of a Canadian secret intelligence service? The issue seems to centre on the notion of 'image'. That image, however, is somewhat misleading, given our use of intelligence obtained by the espionage services of other countries.

**74.** It is difficult to gauge the political costs incurred by democratic countries who do deploy secret services. Unquestionably, as the recent situation in Iran vividly demonstrates, the conduct of secret intelligence activities abroad can have dire effects on a country's international relations and the security of its citizens. Risks of this kind can be reduced but not eliminated by confining a foreign intelligence agency to the collection of intelligence and denying it any mandate for political intervention or para-military operations.

**75.** There is also a serious moral issue involved in a government employing a secret agency whose *modus operandi* requires it necessarily to break the laws of other nations. It may be argued that the existence of an agency with such a mandate brings with it a risk of influencing the practices of a country's security intelligence agency. Lawbreaking can become contagious both within a country's 'intelligence community' and amongst those senior officials of government and the national political leaders who are responsible for directing the intelligence community. Were this to happen in Canada it could seriously undermine reforms which we hope will be put in place to guard against illegality and impropriety in the activities of the security intelligence agency and the R.C.M.P. On the other hand, it may be argued that so long as this risk is recognized, and the proper controls are in effect, the risk of such influence and contagion can be minimized.

**76.** We do not know the extent to which Canada's abstaining from foreign espionage has been based on moral or political considerations. It may have been based more on a judgment that Canada's allies provide so much intelli-

gence to this country that our basic foreign intelligence requirements can be met from these sources. Whether or not this is a correct interpretation of past policy, we do not know. However, we do believe that a careful analysis of the various costs and benefits is overdue and that a review should be carried out so that Canada's policy on this particular feature of its intelligence capabilities might be decided upon in an informed and mature manner. In urging that there be further study of this matter we emphasize that we are referring only to the *collection of intelligence*; we are not in any way suggesting that the Canadian government should even examine whether or not it should have a service which may be used to destabilize foreign governments or attack their leaders.

*Organizational and governmental aspects*

**77.** While we make no recommendations either for or against the establishment of a secret foreign intelligence service, we do think it important to indicate how, organizationally and in terms of government direction, such a service should relate to a security intelligence agency.

**78.** In our view, it would be extremely important to keep such an agency separate from the security intelligence agency. We have already mentioned the dangers of contagion with respect to an espionage agency's practice of violating the laws of other countries. Further, it is clear to us that the intelligence which such an agency collects would go well beyond the purposes of security intelligence. It would be unwise to combine very different intelligence collection responsibilities within a single agency. In addition, there is a danger of creating a security and intelligence monolith in a democratic state. Demarcation lines between the two services, dealing with the foreign and domestic overlap of the two, would have to be carefully drawn.[2]

**79.** If a foreign intelligence agency were to be established by Canada it should not be done in the surreptitious fashion in which such agencies have been established in other countries. In the western democracies we have surely learned by now the need to subject intelligence agencies to the basic precepts of democratic and responsible government. This means at the very least that a Canadian foreign intelligence agency should have a clear charter approved by Parliament. While working out a legislative mandate is not without difficulty, the task should be easier than recent American experience indicates, for in that country the biggest difficulties have centered on notification of Congressional Committees, and approval of covert operations involving political interference in the affairs of foreign countries, rather than on intelligence collection. As a Canadian service should not have a mandate to indulge in active measures of intervention, drawing up a charter to cover the collection of secret intelligence might be somewhat less complicated and controversial. In addition to a prohibition on active measures, we would not envisage a secret service having any paramilitary functions.

[2] See, for example, John Bruce Lockhart, "Secret Services and Democracy", *Brassey Annual Review*, 1975-76; and "The Relationship Between Secret Services and Government in a Modern State", *Journal of the Royal United Services Institute for Defence Studies*, June 1974.

**80.** A legislative mandate should also specify the controls to which such a service would be subjected and also provide for Executive and Parliamentary review of its activities.

**81.** Finally, it is almost axiomatic that the government should develop an assessment capacity not solely within the collecting agency. Recent experiences abroad amply illustrate the dangers of maintaining the two functions wholly within one agency. Thus the establishment of a strengthened capacity at the centre of government for assessing intelligence and defining intelligence priorities along the lines proposed in Part VIII of this Report would be an essential prerequisite for an expanded foreign intelligence collection capability.

# CHAPTER 8

# RELATIONSHIPS WITH OTHER DEPARTMENTS PROVINCIAL AND MUNICIPAL AUTHORITIES

## INTRODUCTION

**1.** In this chapter, we examine the relationship of the security intelligence agency with other governmental bodies having security and intelligence responsibilities. The chapter has two sections. In the first, we focus on what some refer to as the federal government's 'security community'. We concentrate most of our attention on two departments — the Department of External Affairs and the Department of National Defence. Other departments are also affected by our recommendations but in this chapter we indicate only the general nature of these changes and where they are dealt with in this Report. In the second section of this chapter, we explain the relationships between the security intelligence agency and provincial and municipal authorities. Our general theme throughout both parts of this chapter is the need for a higher degree of co-operation among those government bodies whose activities in some way affect the security of Canada.

## A. RELATIONSHIPS WITH OTHER FEDERAL GOVERNMENT DEPARTMENTS AND AGENCIES

**2.** In earlier chapters of this Report, we noted that the R.C.M.P. has made formalized written agreements with a significant number of federal government departments and agencies. Many of these agreements have sections relating to the Security Service. We have expressed our concern, particularly in several chapters in Part III, with the contents of some of these agreements. Here, we wish to register our deep concern over the fact that most of these agreements were not submitted for approval by the Solicitor General, the Minister responsible for the R.C.M.P. These agreements do not deal with trivial matters; many have an important bearing on significant policy issues affecting R.C.M.P. operations. Moreover, as we pointed out earlier, some of these agreements are questionable on grounds of legality and propriety. We believe that the Deputy Solicitor General and the Director General of the security intelligence agency should ensure that all agreements which are made between the agency and other federal government bodies and have significant implications for the conduct of security intelligence activities be brought to the

attention of the Solicitor General for his approval. The Solicitor General should inform his colleagues on the Cabinet Committee on Security and Intelligence of the nature of these agreements.

**3.** The unwillingness on the part of the R.C.M.P. to seek the Solicitor General's approval of agreements with other departments is another manifestation of one of the Force's principal weaknesses: its poor capacity for dealing effectively with other departments and agencies of government. Nowhere is this weakness more apparent than in the Security Service's relationship with the Department of External Affairs.

*The Department of External Affairs*

**4.** As we have stated throughout this Report, many of the threats to Canada's security emanate from abroad. This single fact demands the closest of co-operation between the Department of External Affairs and the security intelligence agency. Until recently, however, they have not enjoyed a close relationship. In some ways, the tension and suspicion between the two bodies is almost inevitable: the Department of External Affairs is committed to an easing of international tensions based on co-operation and understanding; the Security Service tends to view the activities of many foreign countries with deep suspicion. The result is a difference of views on the threats to this country's security which originate abroad. One example of how these differing points of view lead to conflict is in deciding the appropriate course of action in the case of a foreign diplomat engaging in improper intelligence activities. While the Security Service has generally favoured the prompt expulsion of these diplomats, the Department of External Affairs, either through fear that Canadian diplomats will be expelled in reprisal or because of the timing of a certain diplomatic initiative, has not always agreed to declare these diplomats *personae non gratae*. Such differences, we should note, are not peculiar to Canada. In the nations with which we are most familiar, similar tensions exist between those organizations charged with the conduct of foreign relations and those concerned with the conduct of security and intelligence activities. The situation in this country, however, is worse than it needs to be, in part because of the wide differences in educational background and work experiences of the staff of the two organizations. We think that some of our recommendations will help this situation, principally those dealing with the recruitment and training of personnel for the security intelligence agency. Such measures will go some way towards encouraging a greater measure of sophistication in the analysis of international affairs by the agency, a change that in itself we would hope will reduce the current disparities in the views of the Department of External Affairs and the Security Service.

**5.** While mutually negative attitudes have been part of the underlying tension between the two bodies, an attempt has been made by both of them since the mid-1970s to provide mechanisms for improving the process of co-operation.

**6.** We believe that a Memorandum of Understanding is one means of ensuring compatibility between Canada's security intelligence activities — which have international effects — and its foreign policy endeavours. Conse-

quently we recommend that the separate and civilian security intelligence agency, the creation of which we propose in Part VI, draw up a memorandum of understanding between itself and the Department of External Affairs. This document should be prepared by the respective deputy ministers, the Under Secretary of State for External Affairs and the Deputy Solicitor General, and submitted for approval to their Ministers. It should cover the appropriate aspects of security and intelligence co-operation and co-ordination listed above. We now consider the general principles which should be contained in this memorandum. The changes we are recommending call for a higher degree of involvement by the Secretary of State for External Affairs and his officials in setting security intelligence policy and in deciding on specific operations with international implications.

(i) *Consultation*

**7.** There are at present regular meetings between the Deputy Under Secretary of State for External Affairs (Security and Intelligence) and the Director General of the Security Service. We think it would be desirable to continue this practice after the formation of a separate and civilian security intelligence agency. In addition, there is a need for the Deputy Solicitor General and the Under Secretary of State for External Affairs to discuss on a regular basis important questions of policy requiring resolution. The role of the Deputy Solicitor General in these policy discussions is consistent with the recommendations we make in Part VIII, Chapter 1, calling for this official to be more active in directing and controlling the security intelligence agency.

(ii) *Foreign operations undertaken by the security intelligence agency*

**8.** In the previous chapter, we set out the need for a set of guidelines for foreign operations of the security intelligence agency. Further we recommended that the Cabinet Committee on Security and Intelligence, of which the Secretary of State for External Affairs is a member, should approve such guidelines. Under our recommendations, the Solicitor General and his deputy have the main responsibility for ensuring that the guidelines are adhered to by the security intelligence agency. Our recommendations also call for periodic reviews of the guidelines by officials in the Department of External Affairs and the security intelligence agency in the light of past operations. The security intelligence agency should consult with the Department of External Affairs in advance only concerning those foreign operations with significant implications for Canada's foreign relations.

(iii) *Counter-intelligence operations in Canada*

**9.** Counter-intelligence operations in Canada are of concern to the Department of External Affairs when they involve foreign nationals working in this country, or diplomats working out of their missions here who are suspected of intelligence activities. In Chapter 4 of this part of the Report, we discussed information collection methods to be employed by the security intelligence agency. We recommended the establishment of three basic levels of investigation. The third level, what we have called the full investigation, requires a

three-stage initiating procedure. It is at the first stage, in which senior officers of the security intelligence agency and officials of government departments consider the merits of proposals for full investigation, that we think the Department of External Affairs should be consulted in certain circumstances when proposals have a bearing on foreign relations. We should emphasize that External Affairs should not have a power of veto over security operations. (Differences between the security intelligence agency and External Affairs which cannot be resolved at the official level must be taken up at the ministerial level.) Nevertheless, our recommendations here call for a higher degree of involvement of the External Affairs Minister and his officials in important operational decisions.

(iv) *Agreements between the security intelligence agency and foreign agencies*

**10.** Our principal recommendation here, as set out in Part V, Chapter 7, was that future agreements conform to guidelines to be formulated by the Cabinet Committee on Security and Intelligence and approved by Cabinet.

*The Department of National Defence*

**11.** The Department of National Defence has responsibilities to provide "aid of the civil power" under section 233 of the National Defence Act.[1] Under this section, the Chief of the Defence Staff must comply with a request for troops from a provincial attorney general in

> ... any case in which a riot or disturbance of the peace requiring such services occurs, or is, in the opinion of an attorney general, considered as likely to occur, and that is beyond the powers of the civil authority to suppress, prevent or deal with.

The Chief of the Defence Staff has the authority, however, to determine what resources are required to deal with a particular situation. (We discuss "aid of the civil power" in more detail in Part IX, Chapter 1.) To help the Department of National Defence perform these responsibilities, there are arrangements for the exchange of intelligence and information concerning the threat to internal security. It is recognized that the flow of information is primarily one way — from the Security Service to the Department of National Defence.

**12.** Under the mandate we are proposing for Canada's security intelligence agency, there will continue to be a need for close co-operation between the Department of National Defence and the new agency. The Department has other needs for security intelligence information in addition to "aid of the civil power". Securing Canadian Forces bases across the country and being aware of the activities of foreign spies interested in Canada's military secrets are two such examples. We consider it necessary, therefore, that the Deputy Solicitor General, the Deputy Minister of National Defence and the Chief of the Defence Staff negotiate a Memorandum of Understanding to be ratified by their respective Ministers.

[1] National Defence Act, R.S.C. 1970, ch.N-4.

**13.** Our recommendations in Part VII with respect to the security screening process will not significantly alter the Department of National Defence's security screening role in regard to its own employees. The Department would continue to call upon the R.C.M.P. for criminal records checks, and would request information from the security intelligence agency about activities which are threats to security as defined by Parliament. The Department could carry out field investigations, as it now does, provided that these investigations are confined to information about a person's character and personal qualifications and are consistent with the role we have recommended for security staffing officers from the Public Service Commission or government departments. (See Part VII, Chapter 1.)

**14.** As for communications security, the security intelligence agency would continue the Security Service's role of providing technical advice and intelligence about threats to security to all those in government responsible for maintaining communications security. The R.C.M.P.'s "P" Directorate would retain its lead role in establishing and monitoring the maintenance of standards in technical security matters such as in computer security. The Department of National Defence would thus liaise with both "P" Directorate and the security intelligence agency on these matters.

*Other federal government departments and agencies*

**15.** We refer the reader to the appropriate chapters of our Report where our recommendations have important implications for the relationship of the security intelligence agency to other federal government departments and agencies. There are four such chapters. Our recommendations for the security screening of the Public Service in Part VII, Chapter 1 have an important impact on other government departments and especially the Public Service Commission. Then, in Part VII, Chapter 2, where we discuss security screening for immigration purposes, we suggest a number of changes affecting the Canadian Employment and Immigration Commission. In Part VIII, Chapter 1, we examine the interdepartmental security and intelligence committee system, and here again, our recommendations have important implications for several government departments. Finally, in Part IX, Chapter 1 we discuss the subject of crisis management, another area of interdepartmental endeavour for the security intelligence agency. In all of these chapters, our aim is to ensure that the relationships of the agency with other government departments conform to the mandate we are recommending for the agency, help the agency become better integrated with the rest of government, and provide the agency with continuing 'feedback' about the usefulness of the information it is providing.

**WE RECOMMEND THAT the Solicitor General approve all agreements which the security intelligence agency makes with other federal government departments and agencies and which have significant implications for the conduct of security intelligence activities.**

(57)

**WE RECOMMEND THAT the security intelligence agency, once it has separated from the R.C.M.P., negotiate a Memorandum of Understanding with the Department of External Affairs.**

(58)

**WE RECOMMEND THAT the Deputy Solicitor General, the Deputy Minister of National Defence and the Chief of the Defence Staff negotiate a memorandum of understanding to be ratified by their respective Ministers.**

(59)

## B. RELATIONSHIPS WITH PROVINCIAL AND MUNICIPAL AUTHORITIES

**16.** In a federal state, the relationship between federal security authorities and provincial governments and the police forces under their authority is extremely important. Australia and the Federal Republic of Germany are considerably ahead of Canada in establishing an effective system of liaison between the national security agency on the one hand and the governments and police forces of the member states on the other. Granted that each federal state must achieve inter-governmental co-operation according to its own constitutional traditions and institutional arrangements, still we think there is room for much improvement in federal, provincial and municipal liaison on national security matters in Canada. To a large extent we think that improvement in this area depends on recognition by the federal authorities that from a practical point of view Canada's security should not be treated as a water-tight compartment of exclusive federal responsibility and that effective protection against security threats requires the co-operation of provincial and municipal authorities. We develop this theme further in examining the following five areas: security screening, V.I.P. protection, liaison with provincial police and security organizations, co-operation between federal and provincial ministers, and the investigation of criminal activity by members or sources of the security intelligence agency.

*Security screening*

**17.** The provision of security screening services by the R.C.M.P. for provincial and municipal authorities has a long history. Here we summarize briefly only the highlights of this history. In 1954, R.C.M.P. Commissioner Nicholson agreed to undertake 'subversive' and criminal records checks for the police forces that were members of the Chief Constables' Association of Canada. The Ontario Provincial Police and the Metro Toronto Police were the only forces to take advantage of the offer. An R.C.M.P. policy was adopted in 1957, and reaffirmed in 1963, which approved assistance to contract provinces (those provinces that, under arrangements with the federal government, use the R.C.M.P. for policing, both on a provincial and municipal basis) under strict conditions, whereby the provincial attorney general could request background security checks on provincial government employees. An arrangement with a non-contract province occurred in October 1971, when the Quebec Police Force set up screening arrangements with the R.C.M.P. for the Centre d'Archives et Documentation (C.A.D.), a security intelligence advisory Committee for the Quebec government. Under this arrangement the Quebec Police Force did the field investigation and the R.C.M.P. did the criminal and subversive records checks. As requests grew dramatically, the Quebec govern-

ment under Premier Robert Bourassa adopted a screening document similar to the federal government's Cabinet Directive 35 (CD-35), the document setting out security criteria for employment in the federal Public Service. From 1971 to 1977, the Security Service conducted over 6,000 security screening checks on behalf of the Quebec authorities.

**18.** In June 1978, the R.C.M.P. Security Service in South Western Ontario submitted a memorandum seeking clarification of the federal government's policy in relation to the screening of applicants for the Ontario Provincial Police, and the Metro Toronto Police Department, and for sensitive positions within the Ontario government. This request led to a review of the screening service provided by the R.C.M.P. Security Service to police forces and provincial governments, and to an examination of the authorizations for providing this service. Because CD-35 did not specifically authorize screening services for agencies outside of the federal government, the Director General of the Security Service, Mr. Dare, gave instructions on June 29, 1978 to suspend this screening service.

**19.** While the programme was suspended pending the Solicitor General's decision, Mr. Dare, in a letter to Mr. Bourne, the Assistant Deputy Minister, Police and Security Branch, provided two reasons in support of continuing the vetting service. The first was that joint operations between federal, provincial and municipal security and police agencies required close co-operation. Hence, it would be desirable that municipal and provincial participants in these joint operations be security cleared. Second, the screening of some provincial and municipal government employees was defensible on grounds of national security. Employees with access to sensitive information involving, for example, the administration of justice, the vital points programme, or emergency measures, should be "loyal, reliable and of good character". Consequently, Mr. Dare proposed that the R.C.M.P. should respond to (a) requests from an attorney general which had a bearing on national security and (b) requests from a provincial or municipal law enforcement agency which was a member of the Canadian Association of Chiefs of Police. The Honourable Jean-Jacques Blais, the Solicitor General, gave his authorization for a resumption of the screening service on an interim basis. Before the service resumed, however, the government changed and the matter was not acted upon by the new Solicitor General, the Honourable Allan Lawrence. The present Solicitor General, the Honourable Robert Kaplan, has also not authorized the resumption of this service.

**20.** We believe that there are distinct advantages in the security intelligence agency providing security screening services to provincial governments and to provincial and municipal police forces. The provision of such services should improve communication between federal and provincial bodies with security responsibilities and may facilitate further federal-provincial co-operation. In addition, there is a real danger that security intelligence services, established in part to perform this service, will proliferate at the provincial level. Increasing the number of such services in Canada would appear to us to complicate the control and monitoring of security intelligence activities. In recommending that the federal government provide screening services upon request to provincial governments and provincial and municipal police forces, we emphasize that the

Solicitor General should approve all such requests for a screening programme and that the security intelligence agency should provide only information that is within its mandate to collect. Thus, those provincial and municipal bodies receiving the screening services should have primary responsibility for assessing character reliability. Finally, we believe that it would be highly desirable for a province using this screening service either to establish its own review mechanisms for persons who believe that they have been treated unfairly in the screening process, or to 'opt into' the federal review system which we propose in Part VII, Chapter 1.

**21.** What should happen if the security intelligence agency, in the course of an investigation not connected with a provincial screening programme, comes across information relating a provincial public servant or politician to a security threat? In our examination of Security Service files, we discovered that at least one such case had occurred within the last 10 years. A regionally based Security Service officer approached a provincial premier in order to warn him about the activities of certain members of his party. We believe that a security intelligence agency should report security relevant information to provincial politicians and officials, but the agency should exercise great care in doing so. Otherwise, as we noted in Part V, Chapter 3, it runs the risk of damaging the very democratic process which it has been established to secure. Given the sensitivity of such matters, we believe that the agency should seek the approval of the Solicitor General before reporting security relevant information relating to provincial politicians or public servants.

*V.I.P. security*

**22.** A further aspect of security work in which a high degree of federal-provincial co-operation is required is in the protection of V.I.P.s such as members of the Royal Family, the leaders of other countries and Canadian dignitaries. Currently, "P" Directorate of the R.C.M.P. is responsible to the federal government for protecting V.I.P.s, a responsibility that involves liaison with provincial authorities and also with the R.C.M.P. Security Service. The Security Service is expected to provide "P" Directorate with assessments regarding security threats to V.I.P.s including the potential for violence developing at international events taking place in this country. It is not the role of the Security Service to provide the actual protection, but rather the intelligence on which protective measures can be based. It falls to "P" Directorate to produce the actual plans and details of protection. In performing this function, "P" Directorate often must solicit the help of provincial and municipal police forces who will assist in the role of providing protection. In the past, disagreements have arisen either because, in "P" Directorate's view, too much security has been provided or, alternatively, too little has been provided.

**23.** We believe that a more systematic process of co-operation and co-ordination is necessary. In line with some foreign experience, we think that a formal mechanism should be established to co-ordinate V.I.P. security measures. To this end, it would be useful for the government to study the evolution and practice of the co-operative and co-ordinating machinery that exists in Australia and in the Federal Republic of Germany. The recently established

Australian machinery is particularly interesting. In proposing the establishment of a Standing Advisory Committee on Commonwealth-State Co-operation for Protection against Violence, the Australian Prime Minister stated that its purpose was to achieve "the highest degree of efficient operation and co-operation on a nationwide basis"[2] in providing advice to government about politically motivated violence. It meets every six months. In Canada, there now exists federal-provincial-municipal co-ordinating machinery for dealing with various kinds of crises. Similar machinery could be developed for V.I.P. security. One facet of this co-ordinating machinery might be written agreements between various levels of government. These should set out, we think, the duties of the law enforcement agencies and also the role of the security intelligence agency as the collector of intelligence and the body responsible for taking the lead role in assessing the degree of threat. In this way, and with a central body for co-ordination, the degree of overlap between the jurisdictions might be reduced and protective security measures more effectively co-ordinated between them.

*Liaison with police and provincial security organizations*

**24.** V.I.P. protection is only one among many security concerns requiring co-operation between the security intelligence agency and domestic police forces. With the creation of a separate and civilian agency at the federal level, liaison problems may increase at least in the short term, because of the traditional reluctance on the part of police forces to share criminal intelligence information with members of an agency who are not policemen. To help overcome these problems, we make two suggestions. First, the security intelligence agency should establish a special liaison unit, staffed in part by personnel with police backgrounds. The major responsibility of this unit would be to facilitate the exchange of security relevant information with domestic police forces and to encourage co-operation. Second, following the example of its Australian counterpart, the security intelligence agency should attempt to develop written agreements with major domestic police forces. These agreements, among other things, would establish liaison channels, specify the types of information to be exchanged, and indicate under what conditions joint operations could be conducted. The Solicitor General should approve such agreements.

**25.** The potential problems connected with joint operations deserve special comment. The evidence given before us of the joint operation against the A.P.L.Q. (Operation Bricole) by members of the Montreal City Police, the Quebec Police Force, and the R.C.M.P. Security Service illustrates that the planning for this operation took place at the local level in isolation from Security Service Headquarters. Because there was no plan approved by Headquarters, the respective roles of the three forces were unclear. The R.C.M.P. officer who was asked to approve the actual surreptitious entry of A.P.L.Q. offices was under the impression that the R.C.M.P. was playing only a support role. He gave his approval because he believed that, if he failed to do so,

[2] Quoted in Mr. Justice R.M. Hope, *Protective Security Review* (Canberra, 1979), p. 56.

relations between the R.C.M.P. and the two forces would suffer. To avoid these and other problems, we propose that the Director General or a deputy designated by him be informed of all joint operations. Of course, under the control system we have recommended joint operations involving the most intrusive techniques in investigation will also require ministerial approval. Moreover, general schemes of longer term co-operation between the security intelligence agency and provincial authorities should require ministerial approval. Before approving a joint operation the Director General should have at least the following information:

- an assessment of the target
- the reasons for the joint operation
- the resources each partner in the operation plans to commit
- the expected duration
- the organizational structure for the operation
- the type of investigative techniques to be used
- a plan for providing senior members of the security intelligence agency with periodic progress reports

**26.** Even these two types of prior approval may not be sufficient to avoid all of the serious pitfalls that a joint operation may present. For example, we would be concerned if the partners of the security intelligence agency in a joint operation rather than the agency itself took complete responsibility for employing intrusive investigative techniques. In this way, the agency would be receiving the intelligence and indeed participating in the management of the operation without having to go through the stringent control procedures which we have recommended in Chapter 4 of this part of our Report. To avoid this problem, we are of the view that the security intelligence agency should not use joint operations to circumvent control procedures for the use of covert intelligence-gathering methods. The Solicitor General should develop guidelines for the use of such methods in joint operations.

*Relationships with provincial attorneys general and solicitors general*

**27.** Co-operation in the past between federal and provincial authorities with security responsibilities has been of an *ad hoc* nature. We have already noted the situation regarding security screening for provincial or municipal authorities. Co-operation between the two levels of government, has, typically, been through two channels: from the federal Solicitor General to his provincial counterparts; and from the R.C.M.P. to the provincial attorney general. In total, however, there has been little co-operation of a systematic nature. In the autumn of 1977, at the close of the Federal-Provincial Conference of Attorneys General, a press communiqué was issued committing the Ministers responsible for police forces at both levels of government to close co-operation and co-ordination of intelligence-gathering in relation to organized crime. In response to this commitment, the R.C.M.P. canvassed all divisional Commanding Officers on the method and frequency of their communications with provincial attorneys general. The results showed a great diversity in the

frequency of contacts. While these contacts dealt principally with police matters, the Director General of the Security Service, Mr. Dare, directed that briefings of provincial authorities should also cover security matters of mutual concern such as terrorism. The briefings took place in the first half of 1978 and concentrated on areas where the Security Service's application of covert investigative techniques may have contravened provincial statutes. One result was that some of these techniques were discontinued pending clarification of their use by the attorneys general.

**28.** Our philosophy is that a spirit of federal-provincial co-operation should exist in the areas of policing and security. As stated at the beginning of this section, these areas will not benefit from a jealous guarding of jurisdictions. Indeed, many of our proposals are premised upon co-operation between the federal government and the provinces. Unilateral action cannot resolve many of the issues that we have examined throughout this Report. In the preceding paragraphs we have mentioned the need for systematic co-operation between the two levels of government through the use of written agreements covering such activities as security screening, V.I.P. security, and liaison between the security intelligence agency and provincial and municipal police forces. Similar co-operation is necessary in the effective handling of complaints alleging R.C.M.P. misconduct — a topic which we examine in Part X, Chapter 2. In addition, our analysis has shown that if the rule of law is to be strictly observed, neither the security intelligence agency nor criminal investigation agencies can effectively carry out their functions without amendments to provincial as well as federal laws. Thus there is a need for formal co-operation between the federal Solicitor General and the provincial attorneys general or solicitors general in obtaining the necessary legislative changes.

**29.** It is clear, therefore, that for both legal and operational reasons, the Solicitor General and his provincial counterparts should establish more effective procedures and mechanisms for federal-provincial co-operation in security matters. In this regard, we should note one further concern. It would be tragic for the future of Canadian democracy if, having brought security intelligence operations under an adequate system of control at the federal level, there were to emerge at the provincial level or in the private security industry organizations using operational techniques which encroach on liberal democratic principles and which are not subject to a rigorous system of democratic control. We are particularly concerned about the growth of the security industry in the private sector. There are now more private security personnel in Canada than there are policemen. A few large firms dominate the contract part of the industry and within such firms former members of the R.C.M.P. are prominent. There is some evidence that these former members retain close links with their former colleagues — links which may give them access to security information.[3] A prime concern in the expansion of private security forces is their effect on cherished freedoms in this country through, for example, their

[3] The expansion of the security industry in the private sector is outlined in Clifford D. Shearing and Philip C. Stenning, *Private Security and Law Enforcement in Canada*, a study prepared for the Department of the Solicitor General, December 1977.

possible use to infiltrate groups in order to prevent unionization. A similar growth in the private security industry is evident in the United States particularly since the reforms which have changed the scope of F.B.I. operations. We are disturbed by this trend and are convinced that effective co-operation between the federal and provincial authorities, including the security intelligence agency, must be established to monitor this development.

*The reporting and investigation of alleged criminal activity committed by members or agents of the security intelligence agency*

**30.** Two important questions concerning the relationship between federal and provincial governments arise when there is some indication that members or agents of the security intelligence agency have been engaged in acts that may be violations of the Criminal Code or other federal or provincial statutes. First, if knowledge of criminal activity first comes to the attention of the Solicitor General of Canada or some other federal Minister, should they be obliged to bring the matter to the attention of the prosecuting authorities in the province where the violation of the law has apparently occurred? Second, should there be any limitations on the access by provincial investigators to information held by the federal government which may relate to the alleged offences?

**31.** These are difficult questions and neither existing statute law nor judicial decisions provide full answers. These questions have not been submitted to a systematic analysis by provincial and federal authorities, nor are we aware of clearly defined solutions adopted by other federations. We think it will be essential for federal and provincial authorities to discuss these questions and to consider alternative solutions. The approach we suggest below is designed to strike a balance between provincial responsibility for the administration of justice and the paramount federal responsibility for protecting the security of Canada. As such, it avoids the extreme of giving either level of government an absolute and exclusive authority for investigating and directing criminal proceedings with respect to criminal activities by persons associated with the security intelligence agency. We hope that this proposal will be of assistance to those involved in federal-provincial consultations on this subject and we suggest that the approach we outline below be followed at least on an interim basis while a permanent system is being developed.

**32.** We think that the starting point for answering the questions we pose in this section must be recognition of the fact that traditionally in Canada the provinces have exercised the prime responsibility for instituting criminal proceedings. We are not concerned here with violations against the Official Secrets Act, which expressly makes prosecution subject to the approval of the Attorney General of Canada, or with the Narcotic Control Act, as to which the Supreme Court of Canada has held that there is concurrent federal and provincial jurisdiction to prosecute.[4] We also leave aside other federal statutes that create offences, such as the Income Tax Act and the Customs and Excise Act, jurisdiction over the enforcement of which has not in recent years been

[4] *R.* v. *Hauser* [1979] 1 S.C.R. 984.

vigorously asserted by the provinces. As far as federal legislation is concerned our discussion here relates only to violations of the Criminal Code.

**33.** The position traditionally taken by the provinces is that violations of the Criminal Code and of provincial statutes are matters relating to "the administration of justice in the province" and therefore are within provincial jurisdiction under section 92(14) of the British North America Act. There is, of course, no question that the enforcement of provincial statutes is a matter for the provinces. As for the Criminal Code, the provincial position is generally supported by constitutional authorities. One recent author summarizing judicial decisions on this issue states that:[5]

> The responsibility for the enforcement of the criminal law by police and prosecutors has been held to be within the provincial power over the administration of justice.[6] However, the federal Parliament has concurrent authority to provide for the enforcement of the criminal law on the basis that its legislative power over the criminal law (or any other subject matter) carries with it the matching power of enforcement.[7] In fact, however, the enforcement of the criminal law is for the most part carried out by the provinces.

Apart from Supreme Court decisions and statements of constitutional scholars on the law, we take cognizance of the policy statements of federal Ministers of Justice in the House of Commons to the effect that the prime responsibility for instituting proceedings with respect to Criminal Code offences rests with the provincial authorities.[8]

**34.** We see no reason for departing significantly from the tradition of provincial responsibility for criminal proceedings when it comes to offences by persons associated with Canada's security intelligence agency. On the contrary, precluding provincial responsibility for criminal law enforcement on the grounds that national security may be involved would conflict with the pattern of federal-provincial co-operation which, as we have recommended throughout this Report, should be the prevailing practice in national security matters.

**35.** Thus, when federal authorities become aware of possible criminal activities by members or agents of the security intelligence agency, the normal situation should be that the matter is brought to the attention of the appropriate provincial attorney general. It would then be up to police forces accountable to the provincial attorney general to proceed with the investigation and up to the provincial attorney general to decide whether or not to prosecute. We take exactly the same approach to the investigation and prosecution of criminal activity by members of the R.C.M.P. involved in criminal investigation work (see Part X, Chapter 2).

---

[5] Hogg, *Constitution of Canada*, Toronto, Carswell, 1977, pp. 277-8.

[6] Citing principally *Di Iorio* v. *Montreal Jail Warden* (1977) 73 D.L.R. (3d) 491 (Sup. Ct. Can.).

[7] Citing *Re Collins and the Queen* [1973] 2 O.R. 301, affirmed without reference to merits [1973] 3 O.R. 672 (Ont. C.A.); *R.* v. *Pelletier* [1974] 4 O.R. (2d) 677 (Ont. C.A.).

[8] These statements are discussed in J.Ll.J. Edwards, *Ministerial Responsibility for National Security*, Ottawa, 1980, pp. 14-15.

**36.** We think that the proper channel for communicating information to the provincial authorities about criminal activity by members or agents of the security intelligence agency is the Attorney General of Canada. Where federal authorities, such as the Legal Adviser to the security intelligence agency, or the Solicitor General as the Minister responsible for the agency, or the independent review body, (the Advisory Council on Security Intelligence which we recommend be established in Part VIII, Chapter 2), come across evidence pointing to criminal violations by members of the agency or by persons on behalf of the agency, they should bring the matter and *all* the evidence, pertaining to it to the attention of the Attorney General of Canada.

**37.** Once evidence of a criminal offence by a member or agent of the security intelligence agency is brought to the attention of the federal Attorney General, he should, subject to one exception, report the matter and the evidence pertaining to it to the attorney general of the province in which the alleged offence occurred. The one exception is a situation in which the Attorney General of Canada is convinced that national security, as defined in the Act governing the security agency, would be seriously damaged by turning over to the provincial authorites the evidence on which a decision to prosecute would have to be based. Such a decision by the Attorney General of Canada would be subject to a review procedure we will describe below. We stress that a decision not to report evidence of criminal activity to a provincial attorney general should only be made in highly exceptional circumstances by the law officer of the Crown at the federal level, applying the definition of national security in the statute governing the security intelligence agency and subject to an independent review process. The normal situation should be that such evidence is reported to the provincial attorney general so that the conduct of any ensuing investigation and the decision as to whether or not to lay charges may be made at the provincial level. This does not preclude federal authorities, including representatives of the security intelligence agency, discussing with the provincial attorney general the security implications of instituting criminal proceedings. But the decision as to whether or not to prosecute would normally be made by the provincial attorney general.

**38.** The second question we are concerned with may arise when, independently of reports from the federal Attorney General, the provincial attorney general receives information about a possible criminal offence by a member or agent of the federal security intelligence agency. What access will the provincial attorney general have to relevant information held by departments or agencies of the federal government? Let us be clear that we are discussing this question at the investigatory stage. Once a decision to prosecute is made and the case is before the courts, there are a number of laws such as section 41 of the Federal Court Act and rules concerning the protection of the identity of sources which may provide a legal basis for not disclosing certain information in judicial proceedings.[9] But we are concerned here with the position of the provincial attorney general before trial when he is trying to determine whether the evidence in his possession justifies laying a charge. At this stage he may well have reason to believe that important evidence which may have a vital bearing on the exercise of his prosecutorial discretion is in the hands of the federal

government. In these circumstances should there be any limitation on his access to information held by the federal government?

**39.** Again our answer to this question is that, in a situation of this kind, the governing principle should be that the federal authorities co-operate fully with the provincial attorney general and that, subject to one exception, the Attorney General of Canada should see to it that all the information possessed by the federal government pertinent to the alleged offence is disclosed to the provincial attorney general. The one exception to this principle of full disclosure is that there may be very exceptional circumstances in which the disclosure of certain information to provincial prosecutorial authorities would jeopardize the protection of national security as we have defined that concept in this Report. In these circumstances, and subject to a review process which we will enlarge upon below, we think the Attorney General of Canada should have the right to withhold information from a provincial attorney general. Recognition of this right is a necessary safeguard to ensure that the federal government can effectively discharge its paramount responsibility for protecting the security of Canada.

**40.** Setting some limit to the federal government's obligation to co-operate with provincial authorities in investigating criminal activity by members of the security intelligence agency is consonant with the basic tendency in our legal system to balance the need for effective law enforcement with the need to protect other important social values. The powers of investigating and prosecuting authorities in the Canadian legal system are not unlimited. For example, there is recognition at both the investigative and trial stages of our criminal justice system of the need to maintain the confidentiality of lawyer-client communications and, in the public sphere, section 41 of the Federal Court Act recognizes the right of a federal Minister to withhold information from court proceedings on a number of grounds including the danger of causing injury to national security. It would seem to us to be imprudent not to provide some protection for that latter interest at the investigatory stage of criminal proceedings. In taking this position, we should re-emphasize that the limit on provincial investigators' access to federal government information should apply only in exceptional circumstances.

---

[9] In our First Report, *Security and Information* (Ottawa, Department of Supply and Services, 1979), we recommended that "the provision of section 41(2) of the Federal Court Act not apply to security and intelligence documents or their contents and that new legislation be enacted providing that

(a) when a Minister of the Crown claims a privilege for such information on the grounds that its disclosure would be injurious to the security of Canada; or

(b) any person hearing any judicial proceedings is of the opinion that the giving of any evidence would be injurious to the security of Canada

the matter shall be referred to a judge of the Federal Court of Canada, designated by the Chief Justice of that court, to determine whether the giving of such evidence should be refused.

**41.** In a régime which strives to maintain federal-provincial co-operation in security matters such a restriction should rarely apply. But we can think of possible examples. For instance, some information on the security intelligence agency's files will have been obtained from foreign agencies on the firm understanding that it not be passed on to a third party. In the previous chapter we pointed out how essential it was for Canada's security intelligence agency to attach similar restrictions on information the Canadian agency provides to the national security agencies of other countries. We would think it wrong for the federal government to be required to turn over information to provincial investigators in circumstances that would violate the conditions under which information has been obtained from a foreign country. Another example is one in which the identity of a security intelligence informant who has penetrated a terrorist cell may be contained in records of security operations relating to a criminal offence which is being investigated by provincial authorities.

**42.** It is important that the federal decision not to report evidence of criminal activity to a provincial attorney general or to restrict the provincial attorney general's access to information be made as carefully as possible and be subject to review. Therefore, the Attorney General of Canada, as the Law Officer of the Crown at the federal level, should be responsible for making such decisions. He should be guided by a statutory standard which empowers him to withhold information if in his opinion disclosure of the information would seriously jeopardize the protection of Canada's national security as that concept is defined in the Act governing the security intelligence agency. In exercising his judgment the Attorney General of Canada should bear in mind that the governing principle favours co-operation with the provincial attorney general.

**43.** An independent review of the Attorney General's decision should be provided by the independent review body (the Advisory Council on Security and Intelligence). Full details of the information withheld should be reported to that body and, if it does not agree with the decision, it should so notify the Attorney General of Canada, and the Joint Parliamentary Committee on Security and Intelligence.

**44.** To increase the acceptability of the review process to the provinces, we think it would be wise to add provincial representatives to the Advisory Council on Security and Intelligence when it is reviewing decisions of the Attorney General of Canada. For this purpose the federal government should be able to supplement the membership of A.C.S.I. by three persons selected from a panel of seven persons nominated jointly by all the provincial attorneys general. Those persons should be bound by the same constraints as the regular members of the independent review body and therefore would not be permitted to disclose the information to which they are made privy, except to those persons to whom the independent review body may disclose it. We think that, even if the regular members of the independent review body do not decide that the matter should be the subject of comment and report to the Parliamentary Committee, it should nevertheless be the subject of such comment and report if such is desired by a majority of the provincial nominees.

**WE RECOMMEND THAT the security intelligence agency and the R.C.M.P., with the approval of the Solicitor General, provide, upon request, security screening services**

**(a) to provincial governments for public service positions which have a bearing on the security of Canada;**

**(b) to provincial or municipal police forces.**

(60)

**WE RECOMMEND THAT the security screening services provided by the security intelligence agency for provinces and municipalities be subject to the same conditions which apply to the screening services for federal government departments and agencies.**

(61)

**WE RECOMMEND THAT, if the security intelligence agency obtains security relevant information about provincial politicians or public servants in the course of an investigation unrelated to a security screening programme for the Province in question, then the agency seek the approval of the Solicitor General before reporting this information to the appropriate provincial politician or official.**

(62)

**WE RECOMMEND THAT the Solicitor General encourage a provincial government which uses these security sceening services either to establish its own review procedures for security screening purposes or to opt into the federal government's review system.**

(63)

**WE RECOMMEND THAT the Solicitor General initiate a study of V.I.P. protection in foreign countries with federal systems of government with the aim of improving federal-provincial co-operation in this country.**

(64)

**WE RECOMMEND THAT the security intelligence agency, to facilitate the exchange of security relevant information with domestic police forces and generally to encourge co-operation,**

**(a) establish a special liaison unit for domestic police forces, staffed, in part, by personnel with police experience;**

**(b) develop written agreements with the major domestic police forces to include, among other things, the types of information to be exchanged, the liaison channels for effecting this exchange, and the conditions under which joint operations should be conducted.**

(65)

**WE RECOMMEND THAT the Director General approve all joint operations undertaken by the security intelligence agency and that the Solicitor General develop guidelines for the use and approval of intrusive investigative techniques in joint operations.**

(66)

**WE RECOMMEND THAT the Solicitor General develop in conjunction with his provincial counterparts a mechanism for monitoring the use by private security forces of investigative or other techniques which encroach on individual privacy, freedom of association, and other liberal democratic values.**

(67)

WE RECOMMEND THAT

(a) **the federal government immediately initiate discussion with the provinces on the procedures which should apply to the reporting and investigation of criminal activity committed by members or agents of the security intelligence agency; and**

(b) **the arrangements outlined in this chapter be followed on an interim basis.**

(68)