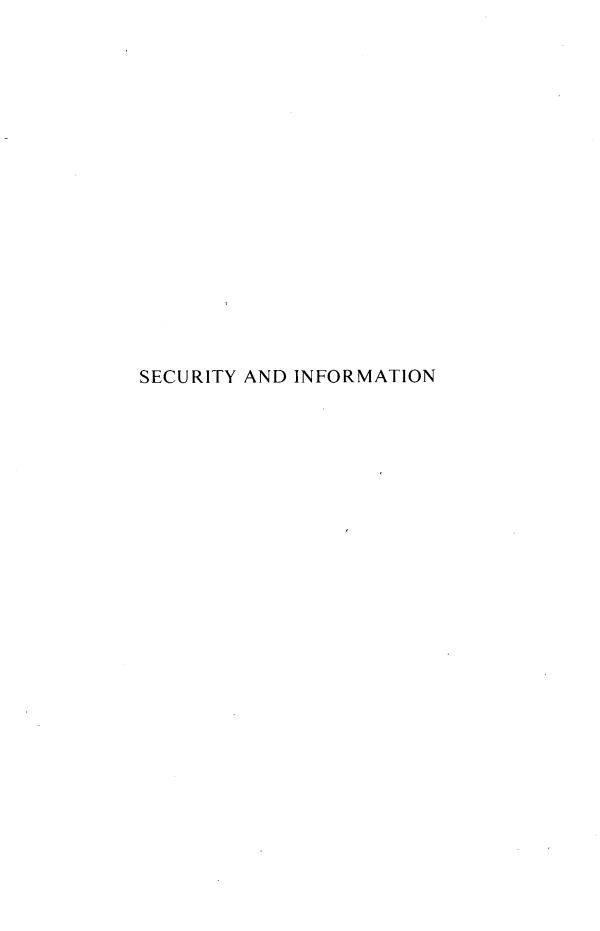


Commission of Inquiry
Concerning Certain Activities of the
Royal Canadian Mounted Police

## First Report

# Security and Information

October 9, 1979



. ţ



## COMMISSION OF INQUIRY CONCERNING CERTAIN ACTIVITIES OF THE ROYAL CANADIAN MOUNTED POLICE

### First Report

## SECURITY AND INFORMATION

#### © Minister of Supply and Services Canada 1980

Available in Canada through

Authorized Bookstore Agents and other bookstores

or by mail from

Canadian Government Publishing Centre Supply and Services Canada Hull, Quebec, Canada K1A 0S9

Catalogue No. CP32-37/1980-1E

ISBN 0-660-10493-8

Canada: \$5.95

Other Countries: \$7.15

Price subject to change without notice

## TO HIS EXCELLENCY THE GOVERNOR GENERAL IN COUNCIL

#### MAY IT PLEASE YOUR EXCELLENCY

We, the Commissioners appointed by Order in Council P.C. 1977-1911 dated 6th July, 1977, to inquire into and report upon certain activities of the Royal Canadian Mounted Police,

BEG TO SUBMIT TO YOUR EXCELLENCY THIS FIRST REPORT ENTITLED: "SECURITY AND INFORMATION"

18000000

Mr. Justice D.C. McDonald (Chairman)

Donald S. Richard

D.S. Rickerd, Q.C.

G. Gilbert, Q.C.

### Table of Contents

		Page
Foreword		ix
THE OFFICI	AL SECRETS ACT	
Introduction .		1
Part I:	BACKGROUND	3
	A. Legislative History	3
	B. Enforcement of the 1939 Official Secrets Act	4
Part II:	LEGISLATIVE REFORM	9
Part III:	SCOPE OF ESPIONAGE	11
Part IV:	COMMUNICATING TO A FOREIGN POWER INFORMATION PREJUDICIAL TO THE SECURITY OF THE STATE	
Part V:	OTHER ESPIONAGE OFFENCES	17
	A: "Prohibited Place"	17
	B. Harbouring	18
	C. Possession of Espionage Instruments	18
	D. Secret Foreign Agents	19
Part VI:	LEAKAGE	21
Part VII:	SOME GENERAL ISSUES	29
	A. Attorney General's Fiat	29
	B. In Camera Trials	29
	C. Procedure for Trying the Cases	32
	D. Penalties	33
	E. Presumptions and Attempts	33
	F. The Applicability of the Law	36
	G. Location of the Provisions	36

EDEEDOM (	OF INFORMATION	Page
	T INFORMATION	39
Part I:	PROTECTION OF SECURITY AND INTELLIGENCE INFORMATION FROM DISCLOSURE UNDER FREEDOM OF INFORMATION LEGISLATION	41
	A. The Competing Interests	41
	B. Protecting those Interests Affected by Non-Disclosure of Security and Intelligence Information	44
	C. Specific Security and Intelligence Information that should be Protected	45
	D. The Method of Protection of Security and Intelligence Information	46
Part II:	PROTECTION OF ADMINISTRATION OF CRIMINAL JUSTICE INFORMATION FROM DISCLOSURE UNDER FREEDOM OF INFORMATION LEGISLATION	51
Part III:	A TIME LIMIT ON NON-DISCLOSURE OF SECURITY AND INTELLIGENCE INFORMATION	53
Part IV:	REVIEW OF GOVERNMENT DECISIONS	55
Part V:	DISCLOSURE OF SECURITY AND INTELLIGENCE INFORMATION IN THE COURSE OF JUDICIAL PROCEEDINGS	57
Part VI:	DISCLOSURE OF ADMINISTRATION OF JUSTICE INFORMATION IN THE COURSE OF JUDICIAL PROCEEDINGS.	61
CONCLUSION		63
SUMMARY	OF RECOMMENDATIONS	65
	S	71
		71

#### SECURITY AND INFORMATION

#### Foreword

One of the responsibilities of our Commission, as set out under Part (c) of our terms of reference, is to advise and report on the "adequacy of the laws of Canada as they apply to ... [the] policies and procedures" governing the "activities of the R.C.M.P. . . . in the discharge of its responsibility to protect the security of Canada." In this report we examine the laws which impose criminal sanctions for the disclosure of information whose release may be prejudicial to national security or to the administration of criminal justice. In particular, we have studied the Official Secrets Act, R.S.C. 1970 c. 0-3 and freedom of information legislation as it relates to security and the administration of criminal justice.

The Official Secrets Act, R.S.C., 1970, c. 0-3, has provided the R.C.M.P. with a statutory basis for the investigation and prosecution of persons suspected of having committed espionage and security related offences against the state. Both the 1946 Royal Commission to Investigate the Facts Relating to the Circumstances Surrounding the Communication by Public Officials and Other Persons in Positions of Trust of Secret and Confidential Information to Agents of a Foreign Power (the Taschereau/Kellock Commission) and the 1969 Royal Commission on Security (the Mackenzie Commission) concluded that the Official Secrets Act required some major alterations. Only a few of the recommended statutory changes were ever implemented. The recent prosecutions against both Dr. Alexander Peter Treu and against the Toronto Sun, its publisher Donald Creighton and its editor Peter Worthington, have also been instrumental in drawing public attention to some of the limitations of this Act.

The Government of Canada is currently studying the general question of access to government information and has expressed its intention to introduce freedom of information legislation within the near future. The Official Secrets Act and freedom of information legislation are interrelated in at least two respects. In the first place, freedom of information laws require certain categories of government information to be made available to the public, whereas the "leakage" provisions of the Official Secrets Act make it an offence to disclose certain types of government information. Obviously there must be consistency between the provisions of freedom of information legislation and the offences prescribed for the unauthorized disclosure of government information. Second, the Official Secrets Act has been the subject of much criticism for having created what is considered to be an unnecessary climate of secrecy. Thus, its reform may be regarded as a necessary element in increasing accessibility to government information. For these reasons, we are reporting on

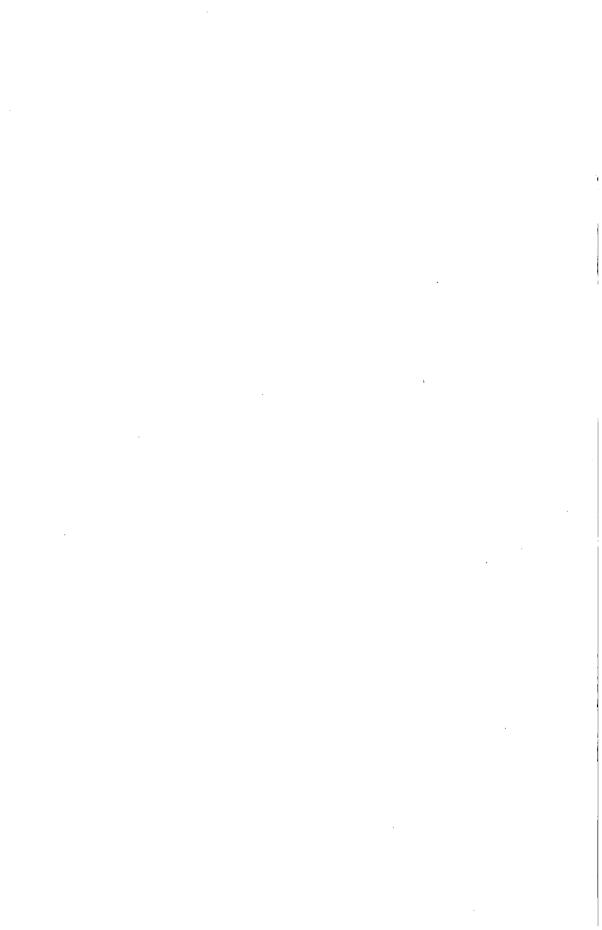
, some aspects of the Official Secrets Act and are making recommendations for substantial revision of this statute. We have also considered the impact of freedom of information legislation on the security of Canada and the administration of criminal justice.

We have not addressed in this report the important issues relating to search and seizure and the interception and seizure of communications which arise out of two separate provisions of the Official Secrets Act and which have been the subject of a good deal of evidence before the Commission. These questions will be discussed at length in a later report.

#### THE OFFICIAL SECRETS ACT

#### Introduction

- The Official Secrets Act, R.S.C. 1970, c. 0-3, has been the subject of widespread criticism for a number of years. The Taschereau/Kellock Commission set up in 1946 following the Gouzenko revelations recommended that the Act be "studied in the light of the information contained" in its report and proceedings, "and, if thought advisable, that it be amended to provide additional safeguards." (page 689) As a result of this report, a number of relatively minor changes were made in 1950. The 1969 Mackenzie Commission accurately described the Act as "an unwieldy statute, couched in very broad and ambiguous language" and concluded that "consideration should be given to a complete revision of the Canadian Official Secrets Act." (page 75) The court in the recent Toronto Sun preliminary inquiry also commented that a "complete redrafting of the Canadian Official Secrets Act seems appropriate and necessary." In 1973, the provision governing the authorized interception and seizure of communications for national security purposes (section 16) was added to the Official Secrets Act although it is arguable that this provision might have been more appropriately placed in the Criminal Code. The "complete revision" of the Official Secrets Act, which was contemplated by the Mackenzie Commission never materialized and many of the concepts and much of the language of the British Official Secrets Acts of 1911 and 1920 remain an integral part of our Canadian Act.
- 2. The Act is complicated by the fact that it deals with two separate, although sometimes related, concepts espionage (section 3) and "leakage," that is the improper disclosure of government information (section 4). In recent years, the leakage provisions have proved to be the principal source of critical comment. The prosecutions against Treu and against the Toronto Sun and its publisher and editor involved the leakage section. Considerable criticism has also been levelled at the comparable provisions in the British legislation. Such expressions of concern in Britain led to the creation of a Departmental Committee under the chairmanship of Lord Franks which conducted extensive hearings on the subject and issued a report in 1972 recommending a number of statutory changes. On the basis of this report the British government in July, 1978 published a White Paper on Reform of section 2 of the Official Secrets Act of 1911.



#### Part I:

#### **BACKGROUND**

#### A. Legislative History

- 3. Concern over the repercussions from a series of incidents which occurred during the 1880s and which involved the improper use of secret government information prompted the British government to pass the first Official Secrets Act in 1889. In 1878, for example, a disgruntled clerk by the name of Marvin divulged to a newspaper for compensation the contents of a secret Anglo-Russian treaty concerning the Congress of Berlin. He was charged with stealing the paper upon which the treaty had been written but because he had only memorized the treaty the prosecution was unsuccessful. A statute, virtually identical to the British Official Secrets Act, was enacted in Canada in 1890. The Canadian Act was transferred to the first Canadian Criminal Code two years later in 1892. These provisions remained in the Criminal Code until their repeal in 1939.
- 4. As the First World War approached, it became increasingly apparent that the espionage sections of the British Act provided insufficient safeguards against the activities of German agents who were "holidaying" in England and photographing harbours and other strategic, though not technically prohibited, areas. Moreover, it was thought to be too difficult to prove under the 1889 Act that an accused possessed information with the intention of communicating it to a foreign state or to any agent of a foreign state. In 1911, a new Act was passed with very little parliamentary debate, although it had been the subject of prior intensive study by the government. As the Franks Committee stated "[The] House of Commons took half an hour to pass the 1911 Bill through all its stages, but the long series of official files recording the events leading up to this legislation stretches well back into the 19th century" (page 23). The Act created a number of presumptions in favour of the Crown which related to the offence of assisting a foreign state. It also made it an offence, with a three year minimum penalty, to obtain or communicate "any ... information which-... might be ... useful to an enemy" (section 1(1)(c)). This provision was designed to prevent Germans from openly obtaining strategic information. Important changes were made in the espionage provisions and the anti-leakage section was broadened so that receipt of official information became an offence. This 1911 extension of criminal liability to the recipient of official information, which most frequently affects members of the press, has proved to be the most controversial section of the Act.
- 5. The 1911 British Act also specified that its provisions should apply to the Dominions overseas. It thus became part of the law of Canada and appeared

the following year in the Statutes of Canada in a list of Imperial Acts that were applicable to this country.

- 6. After the First World War, the British government introduced further changes to the Official Secrets Act, particularly with respect to espionage, which would make permanent certain wartime Defence of the Realm Regulations which the government wished to preserve in peacetime. It was against a background of great social unrest that the British Act of 1920 was enacted. The threat of communism loomed menacingly after the Russian Revolution and the renewed activities of the I.R.A. brought the possibility of civil war in Ireland perilously close. The main debate on the 1920 legislation took place shortly after Bloody Sunday when I.R.A. terrorists assassinated fifteen British intelligence officers in Dublin. The Act was actually introduced at a time when the streets of London were blockaded.
- 7. During the passage of the 1920 statute through the British Parliament, the Attorney General moved an amendment that it not apply to several of the Dominions, including Canada. As he stated "It is not being applied to the Dominions or to India because the Dominions and India have under contemplation legislation which goes somewhat further." (Hansard 1920, Vol. 12, col. 969) No such legislation, however, was introduced by the Canadian government at that time.
- 8. Until Canada enacted its Official Secrets Act in 1939, it was governed by the 1911 English legislation and the analogous provisions which had been introduced into the Criminal Code in 1892 which had not yet been repealed. The 1939 Canadian legislation combined the 1911 and the 1920 British Acts into one act. The Minister of Justice, Ernest Lapointe, in introducing the legislation in the House of Commons on April 12, 1939, stated that "the purpose of the Bill is to consolidate the two Acts and, by an Act of the Parliament of Canada, make them the law of this country." (Hansard 1939, page 2705) Several minor amendments were made in 1950 and again in 1967. The 1970 revision of the statutes incorporated some stylistic changes. As noted above, in 1973 section 16 dealing with the interception and seizure of communications was enacted.

#### B. Enforcement of the 1939 Official Secrets Act

- 9. Well over half of the Canadian prosecutions under the Official Secrets Act arose as a result of the defection of Igor Gouzenko in 1946 and his revelations about a series of spy rings operating in Canada. Almost all of these prosecutions were instituted under the espionage section of the Act (section 3), although the leakage section (section 4) was used alone in one case and as an additional count in another. Many of the prosecutions also involved charges of conspiracy to breach the Official Secrets Act which were brought under the Criminal Code.
- 10. Since the Gouzenko revelations only the following four cases have been tried in Canada under the Official Secrets Act: Biernacki in 1961, Featherstone in 1967, Treu in 1978, and Toronto Sun, Creighton and Worthington in

- 1978.2 The latter two involved prosecutions under the leakage section of the Act.
- 11. The Biernacki case dealt with the important issue as to what type of information is covered by the Act. Biernacki was a landed immigrant from Poland who was collecting information which might be useful in developing espionage activities in Canada. To this end, he had collected data about residents in Canada of Polish birth or extraction. He was charged with five counts under section 3, the espionage section of the Act. The last two counts involved section 9, the attempt section. This case was dismissed at the preliminary inquiry on the basis that the kind of information Biernacki had been amassing was not of the type envisaged by the Act since such information was non-governmental and in the public domain. Furthermore, it was decided that Biernacki's activities had not gone far enough to constitute an attempt under section 9.
- 12. Featherstone was convicted under section 3, the espionage section, and sentenced to two and one half years for trying to pass secret marine charts to the Russians. The charts showed the position of various shipwrecks lying off the east coast of Canada. This would have constituted valuable information for any foreign government wishing to hide its submarines beside the wrecks so as to avoid detection.
- 13. Treu was charged with two counts under the Official Secrets Act for the illegal retention of documents (section 4(1)(c)) and for the failure to take reasonable care of the documents (section 4(1)(d)). The documents, which contained information relating to NATO's secret air defence communication system, had been obtained by him during his term of employment with Northern Electric Co. Ltd. He was tried and convicted, after an *in camera* hearing, and sentenced to two years on the first count and one year concurrent on the second. Treu appealed both conviction and sentence to the Quebec Court of Appeal. On February 20, 1979, that Court unanimously set aside the conviction and entered an acquittal because on the whole of the evidence there was a reasonable doubt. The Court of Appeal did not examine the secret material produced at the *in camera* trial because "the contents were largely irrelevant. What mattered was the Appellant's state of mind, and not the technical data which ... was set out in the exhibits" (per Kaufman, J.A.).
- 13A. There has been considerable discussion in the news media and public criticism of the recent "persecution" of Treu. The public record, however, fails to tell the whole story. In August, 1973, the Security Service learned that Treu was personally responsible for the tender to the People's Republic of China in Hong Kong of a prospectus which contained much secret technical, scientific and military information relating to NATO's air defence communication and surveillance systems. In November, 1973, the R.C.M.P. requested a legal opinion of the Department of Justice as to the likelihood of a successful prosecution of Treu under the Official Secrets Act. According to the Department of Justice, Treu admitted in a statement in March, 1974, that he had prepared the prospectus and had been instrumental in having it relayed to officials of the P.R.C., but that he was under the impression that he was

authorized to do so. Although evidence existed to support a charge under one of the espionage sections [sections 3(1), 4(1)(a) or 4(1)(b)] for the unauthorized communication or use of classified information in a manner prejudicial to the interests of national security, the Department of Justice decided against recommending the prosecution of Treu under the espionage provisions because of the refusal of certain key witnesses to testify. On the basis of representations submitted to him in writing by the Department of Justice, the Attorney General of Canada decided, as required under section 12 of the Act, to prosecute Treu under two of the "leakage" sections [sections 4(1)(c) and 4(1)(d)] for the illegal retention of and failure to take reasonable care of classified information. In its recommendation to the Attorney General the Department suggested that particular consideration be given to two factors. The first was the desirability of taking appropriate action to protect the security of NATO documents to avoid jeopardizing Canada's relationships with other NATO countries. The second factor was the necessity of reinforcing adherence to proper security procedures by persons handling classified official

- 14. An aspect of the proceedings which contributed to the public notion that Treu was being unfairly harassed was the fact that the trial was conducted in camera. Mr. Justice Kaufman stated in his reasons for judgment in the Court of Appeal that the "sense of mystery" surrounding the case was thereby "immeasurably heightened." It should be pointed out that when the Crown applied to the trial judge for an order that the trial be conducted in camera, counsel for Treu advised the court that he had no representations to make on the application. The position of Treu's counsel was given very limited press coverage. It can therefore be seen how the public received the mistaken impression that Treu had become the unwitting victim of a deliberate "persecution" on the part of the government.
- 15. The most recent case involved publication by the Toronto Sun of a document classified as "top secret" which outlined suspected Russian espionage activity in Canada. The Toronto Sun and its publisher and editor were charged with the receipt and subsequent publication of a document in contravention of sections 4(1)(a) and 4(3) of the Official Secrets Act. The charges were dismissed at the preliminary inquiry stage on April 23, 1979. The court concluded that the document, if it had ever been secret, was no longer so. Earlier disclosures had "brought the document, now 'shopworn' and no longer secret, into the public domain."
- 16. One aspect of the *Toronto Sun* case, which was the source of much public comment, was the allegedly arbitrary manner in which the Attorney General had exercised his discretion in deciding to prosecute under the Official Secrets Act. Although much of the security information contained in the R.C.M.P. document "Canadian Related Activities of the Russian Intelligence Services," which was published by the Toronto Sun had previously been televised in a C.T.V. documentary and had been discussed by Mr. Tom Cossitt in the House of Commons, only the Toronto Sun, its publisher and editor were prosecuted.
- 16A. It was decided by officials of the Department of Justice not to recommend to the Attorney General of Canada that charges be laid against C.T.V.

since all of the information which had been released by the television network was considered to have already become public knowledge. In considering this question, the Department of Justice had divided the contents of the top secret document into sixteen different items. Twelve of these items were regarded as already in the public domain but the other four were still considered to be secret. The C.T.V. programme contained information which was either in the public domain or which was not considered to be prejudicial to national security. The Toronto Sun article, on the other hand, contained information which had not been published previously and which was considered to be prejudicial to security.

- 16B. Unlike C.T.V., Mr. Cossitt had disclosed some of the information contained in the four items still considered to be secret. Although in the opinion of officers of the Department of Justice there was evidence to support a charge against Mr. Cossitt under the Official Secrets Act, it was decided by the Attorney General of Canada, after extensive consultations with the Solicitor General and officials, not to proceed against Mr. Cossitt. According to the Attorney General an important factor was that Mr. Cossitt might be able to rely on the privilege afforded Members of Parliament to give him immunity from prosecution.
- 17. In the following statement in the House of Commons on March 17, 1978, the Attorney General explained why he did not give his consent to a prosecution against Mr. Cossitt:

In the present situation, the hon member for Leeds [Mr. Cossitt] has made statements in the House which must clearly have been based upon highly classified national security information. In my judgment, the hon member's use of the secret information he was not entitled to have was contrary to the national interest. However, by law, his statements cannot constitute the foundation for a prosecution under the Official Secrets Act since it is well established that no charge in a court can be based on any statement made by an hon member in this House.

The hon, member for Leeds did, however, make additional statements. In my view, these statements did not add substantially to what he had already said in the House. There is some doubt as to the extent to which a court would view these statements as being protected by any parliamentary privilege or immunity. The existence of this doubt guides me in my decision whether or not to provide my consent to a prosecution.

The obligation of the Attorney General in deciding whether or not to provide his consent under the Official Secrets Act calls into play the many factors I referred to earlier. In my view, an Attorney General should not provide such a consent unless the case is free from substantial doubt.

Having considered the evidence produced in the investigation to date, and having considered applicable legal and parliamentary principles, I have concluded that I should not consent to a prosecution against the hon. member for Leeds.

(Hansard, March 17, 1978, p. 3882)

- 18. In both the *Treu* and the *Toronto Sun* cases, the Crown prosecutor worked in liaison with R.C.M.P. officers from both Criminal Investigation Branch (C.I.B.) and the Security Service. The stage preparatory to the institution of proceedings by the Justice Department was conducted with the involvement of the Criminal Investigation Branch of the R.C.M.P., which was officially in charge of the investigation. In a later report, we will discuss the responsibilities of the C.I.B. and the Security Service respectively with regard to the investigation of espionage offences.
- 19. It must be noted that many espionage cases are disposed of without instituting a prosecution or, in fact, without the matter ever being brought to the attention of the Department of Justice. If a case involves the participation of foreign agents or members of a diplomatic staff, it may be expedient to resolve the problem through deportation, voluntary departure or a declaration of persona non grata. The persona non grata procedure is instituted by a host government against foreign diplomats whose activities are regarded as unacceptable or whose conduct is seen as unbecoming that normally expected of persons working in the diplomatic field. Since 1959, twenty-one diplomats from the U.S.S.R., Eastern Europe, and the People's Republic of China have been declared personae non gratae as a result of engaging in offensive intelligence activities directed against Canada. In addition, a number of other diplomats from the same countries and from Cuba have been asked less formally to leave, for similar reasons. In such cases the machinery of the Official Secrets Act is not invoked. The decision to declare a diplomat persona non grata is taken by the Secretary of State for External Affairs after receiving information from the Security Service of the R.C.M.P.

ۍ. کن

#### Part II:

#### LEGISLATIVE REFORM

20. Any discussion of the reform of the Official Secrets Act is incomplete without mentioning the relationship of this statute to freedom of information legislation, since each deals with a different aspect of accessibility to government information. A Freedom of Information Act deals with the type of government information which must be released on request. It says nothing about the kind of information which may be released by the government. The Official Secrets Act deals with the improper communication of information which has not already been released. Although the two Acts deal with different concepts, they are interrelated in that the Official Secrets Act creates in the words of the Franks Committee "a general atmosphere of unnecessary secrecy." This point is developed by the 1978 British White Paper which refers to freedom of information laws in its discussion of the Official Secrets Act. The White Paper states:

This White Paper is mainly concerned with the new legislation for the reform of section 2 of the Official Secrets Act 1911 (The Canadian section 4). Strictly speaking, questions of open government do not depend on section 2, which is concerned only with the information that needs to be protected from unauthorized disclosure by criminal sanctions. Nevertheless, the Franks Report suggested ... that there was a link between the two topics and that section 2 had some effect in creating a general aura of secrecy. The Government believes that section 2 in its present form because of its very wide ambit does have an inhibiting effect on openness in government. It is in no doubt that reform of this section is not only a much needed improvement of the criminal law but a necessary preliminary to greater openness in government. (pages 18-19)

The 1977 Canadian Government's Green Paper entitled, "Legislation on Public Access to Government Documents," states that the "broad scope of the Official Secrets Act," amongst other things, "constitutes a substantial disincentive to any public servant releasing government documents to a citizen." (pages 14-15)

21. We are convinced that it is wrong to include offences dealing with espionage and offences dealing with the unauthorized disclosure of government information in the same statute. These offences deal with fundamentally different kinds of behaviour and different levels of threat to the state. Continuation of the Official Secrets Act with both offences under the umbrella of the same legal instrument is inconsistent with the steps being taken in Canada to achieve greater openness in government.

- 22. But much more is needed by way of legislative reform than the mere dismantling of the Official Secrets Act and the recognition of espionage and leakage as separate kinds of offences. The definitions of these offences in the Official Secrets Act leave much to be desired. As our account of the Act's historical background indicates, it is now time for this part of our law to be revised so that it is both clear and in tune with the values and needs of contemporary Canada.
- 23. Our plan of attack in making recommendations for this programme of legislative reform will be to consider how the espionage and leakage offences should be defined, then to discuss certain problems common to both offences and finally to indicate the options for locating these offences in the statutes of Canada.

#### Part III:

#### SCOPE OF ESPIONAGE

- 24. Section 3 of the Act, the "spying" section, provides that:
  - 3. (1) Every person is guilty of an offence under this Act who for any purpose prejudicial to the safety or interests of the State,
    - (a) approaches, inspects, passes over, or is in the neighbourhood of, or enters any prohibited place;
    - (b) makes any sketch, plan, model or note that is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power; or
    - (c) obtains, collects, records, or publishes, or communicates to any other person any secret official code word, or password, or any sketch, plan, model, article, or note, or other document or information that is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power.
- 25. The Official Secrets Act is not the only statute that deals with espionage. Under Part II of the Criminal Code, entitled "Offences against Public Order," section 46(2)(b) provides that:

Everyone commits treason who, in Canada, ...

- (b) without lawful authority, communicates or makes available to an agent of a state other than Canada, military or scientific information or any sketch, plan, model, article, note or document of a military or scientific character that he knows or ought to know may be used by that state for a purpose prejudicial to the safety or defence of Canada.
- 26. It will be noted that the wording of section 46(2)(b) overlaps with section 3(1) of the Official Secrets Act. We can see no reason for maintaining both section 3(1) of the Official Secrets Act and section 46(2)(b) of the Criminal Code.

WE RECOMMEND THAT new espionage legislation incorporate in a single enactment the offences relating to espionage now set out in section 3(1) of the Official Secrets Act and section 42(2)(b) of the Criminal Code.

[Recommendation 1]

27. In passing, we would note that this is not the only section of the Criminal Code which deals with matters relating to national security. Section 52, the sabotage section, makes it an offence to damage or destroy property for a "purpose prejudicial to the safety, security or defence of Canada..." Other offences in the Code which have security overtones include forging or using a forged passport (section 58), the fraudulent use of a certificate of citizenship (section 59), and the offences of speaking seditious words, publishing a seditious libel or being party to a seditious conspiracy (sections 60-62).

#### Part IV:

## COMMUNICATING TO A FOREIGN POWER INFORMATION PREJUDICIAL TO THE SECURITY OF THE STATE

- 28. In considering the wording of offences relating to espionage, we are anxious that the law be expressed clearly and precisely. As with all crimes, the citizen is entitled to know what conduct will render him liable to prosecution. In our view, the Official Secrets Act falls short of the precision that is required in criminal law.
- 29. Furthermore, espionage legislation should deal with communication of information only when the communication is directed to a foreign power. Such communications by their very nature will normally be clandestine. As noted above, offences relating to the leakage of government information should be dealt with in legislation separate from espionage legislation. We discuss such leakage offences later in this report.

## WE RECOMMEND THAT espionage offences apply only to conduct which relates to the communication of information to a foreign power.

[Recommendation 2]

30. It has been pointed out that espionage conducted on behalf of a foreign group, such as a terrorist faction, might not fall within the term "foreign power" used in section 3 of the present Act. This possible omission must be corrected to ensure that all such groups are included in the definition.

WE RECOMMEND THAT new espionage legislation define the term "foreign power" to include a foreign group that has not achieved recognition as an independent state.

[Recommendation 3] ·

31. A key question concerning the Official Secrets Act is whether the espionage section 3(1)(c) should apply only to the communication of information that is "official and secret." Section 3(1)(a) speaks of communicating "any secret official code word, or password, or any sketch, plan, model, article or note, or other document or information." To date, all prosecutions in Canada under section 3 of the Act have been pursuant to section 3(1)(c). The words "secret official" did not appear in Britain in the 1889 or 1911 U.K. Acts. They were, in fact, added by a schedule at the end of the 1920 Act and were referred to in the Act itself as "minor details." No one suggested that by adding these words they were changing the meaning of the 1911 Act. As we know, the 1911 Act was introduced in part to control the activities of German agents who were openly collecting information that was clearly not secret or

- official (e.g. sketching harbours). So it is not at all surprising that in Britain, to quote the Franks Committee, "it is clear that the words 'secret official' qualify only the words 'code word, or password'." (page 125)
- 32. When Canada enacted the Official Secrets Act in 1939, there was no indication that a substantial departure from the 1911 and 1920 English legislation was intended. However, Canadian courts have given a different interpretation to the wording of section 3.
- 33. In the Biernacki case the charge against the accused was dismissed at the preliminary hearing. The information being collected by Biernacki was, according to the judgment, not the type of information contemplated by section 3(1)(c) of the Act. It was held that the words "secret official" qualify not only "code word or password" but also the rest of the clause, e.g. "secret official... information." Similarly, in the Toronto Sun prosecutions, the court assumed that the information had to be secret. In Boyer (1948, one of the Gouzenko cases) and the Commission of Inquiry into Complaints made by George Victor Spencer (1966) the same approach was taken.
- 34. Whichever interpretation is correct, the section should be redrafted to remove the existing doubt as to its interpretation. The problem is that the collation and communication to a foreign power of information accessible to all Canadians may, in certain cases, be prejudicial to our national security. For example, the photographing of pipelines, dams, and harbours could be used by the foreign country for sabotage purposes or for bombing in the event of war. The report of the Commission of Inquiry showed that Spencer had supplied agents of the Soviet Union with names and dates of birth gathered from tombstones in Canadian cemeteries which could be used in the establishment of false identities.
- 35. The Mackenzie Report stated that the ideal act "should protect unclassified information from attempts at collection and dissemination which are prejudicial to the interests of the state or intended to be useful to a foreign power" (page 77). It is not clear whether the reference to "unclassified information" meant only that information which is in the government's possession or whether it included non-governmental information. For our purposes, it is unnecessary to draw a distinction between the two since the communication to a foreign agent of information accessible to the public, such as the "tombstone" information gathered by Spencer, may be as prejudicial to security as the communication to a foreign power of unclassified government information.
- 36. We are convinced that any provision relating to espionage should cover the disclosure of, or an overt act with the intention to disclose, information whether accessible to the public or not, either from government sources or private sources, if disclosure is, or is capable of being, prejudicial to the security of the state. We do feel, however, that the communication of information which is accessible to the public should be a lesser offence than the communication of secret government information.

WE RECOMMEND THAT new espionage legislation cover the disclosure of, or an overt act with the intention to disclose, information whether accessible to the public or not, either from government sources or private sources, if disclosure is, or is capable of being, prejudicial to the security of Canada.

[Recommendation 4]

- 37. The present Act requires the prosecution to prove that the accused acted "for any purpose prejudicial to the safety or interests of the state." The treason section in the Criminal Code, section 46(2)(b), on the other hand, refers to information that may be used by a foreign state "for a purpose prejudicial to the safety or defence of Canada." We think that the language of Section 3 of the Official Secrets Act "the safety or interests of the state" is too broad. We prefer the use of the phrase "the security of Canada."
- 38. In Canada, the term "security of Canada" is synonymous with "national security." While one cannot be exhaustive, "the security of Canada" involves at least two concepts. The first is the need to preserve the territory of our country from attack. The second concept is the need to preserve and maintain the democratic processes of government. Any attempt to subvert those processes by violent means is a threat to the security of Canada.
- 39. If the espionage legislation refers to "the security of Canada," we do not think it necessary to make a distinction between espionage in wartime and espionage in peacetime. In the United States, the 1971 Brown Commission, whose recommendations have not yet been implemented, recommended that in wartime there must be a more extensive definition of espionage than in peacetime. The term "security of Canada," however, seems sufficiently flexible to enable a court to take into consideration the special conditions that apply in wartime when virtually any contact with the enemy is inimical to the security of the state.
- 40. We believe that the phrase "security of Canada," if it is used in the definition of espionage, should be defined with as much precision as is possible so that people will know the kinds of conduct that will subject them to prosecution. On the other hand, as we have said, it is not possible to be exhaustive. Moreover, no matter what detail is added by way of definition, a judge or a jury is going to have to apply the criteria to the facts of a particular case. Yet the definition should go at least as far as identifying the two concepts already mentioned. Perhaps the kind of detail that should be stated is along the lines used in the Australian Security and Intelligence Organization Bill 1979. Its definition of "security," and of several phrases found in that definition, is found in Appendix III. When we report on the functions of a security and intelligence agency for Canada we shall have more to say about the meaning of "the security of Canada."
- 41. To assist in the drafting of the proposed new legislation, we would suggest that the basic clause setting out the offence of espionage read as follows:
  - (a) obtain, collect, record or publish any information with the intent of communicating such information to a foreign power, or
  - (b) communicate information to a foreign power,

No person shall:

if such person knows that the foreign power will or might use such information for a purpose prejudicial to the security of Canada or acts with reckless disregard of the consequences of his actions to the security of Canada.

42. It will be noted that the proposed offence imposes criminal liability when an accused has knowledge that a foreign power might use information for a purpose prejudicial to the security of Canada or acts in a reckless manner heedless that such consequences may result. Although our proposed language includes an objective standard, which would apply in cases in which the accused does not have knowledge of the consequences of his actions, espionage may result in such serious damage to the security of the nation that we feel that such an objective standard is required. On the other hand, we would point out that in s.46(2)(b), the treason section, and in s.212(c), the constructive murder section, of the Criminal Code, an accused may be convicted if he knows or "ought to know" the consequences of his actions. In our opinion, however, the narrower standard of reckless disregard for the consequences is appropriate for the serious offence of espionage.

WE RECOMMEND THAT new espionage legislation include the following basic provision with respect to the offence of espionage:

No person shall:

(a) obtain, collect, record or publish any information with the intent of communicating such information to a foreign power, or

(b) communicate information to a foreign power, if such person knows that the foreign power will or might use such information for a purpose prejudicial to the security of Canada or acts with reckless disregard of the consequences of his actions to the security of Canada.

[Recommendation 5]

#### Part V:

#### OTHER ESPIONAGE OFFENCES

#### A. "Prohibited Place"

- 43. The Act in section 3(1)(a) contains a complicated definition of "prohibited place" and makes it an offence to "approach," "inspect," or even be "in the neighbourhood of" such a place. Generally speaking, "prohibited place" includes defence establishments and places so declared by order of the Governor in Council. There have been no prosecutions in Canada under this section of the Act. The notion of the "prohibited place" was no doubt sensible in 1911 but is it necessary today? We do not think so. The concept of obtaining information for a purpose prejudicial to the security of Canada incorporated in the offence of espionage discussed above, would cover activities related to defence establishments, while the offence of sabotage in the Criminal Code (section 52) would cover damage to property. Section 52 reads as follows:
  - 52. (1) Every one who does a prohibited act for a purpose prejudicial to
    - (a) the safety, security or defence of Canada, or
    - (b) the safety or security of the naval, army or air forces of any state other than Canada that are lawfully present in Canada,

is guilty of an indictable offence and is liable to imprisonment for ten years.

- (2) In this section, "prohibited act" means an act or omission that
- (a) impairs the efficiency or impedes the working of any vessel, vehicle, aircraft, machinery, apparatus or other thing, or
- (b) causes property, by whomsoever it may be owned, to be lost, damaged or destroyed.
- (3) No person does a prohibited act within the meaning of this section by reason only that
  - (a) he stops work as a result of the failure of his employer and himself to agree upon any matter relating to his employment,
  - (b) he stops work as a result of the failure of his employer and a bargaining agent acting on his behalf to agree upon any matter relating to his employment, or
  - (c) he stops work as a result of his taking part in a combination of workmen or employees for their own reasonable protection as workmen or employees.
- (4) No person does a prohibited act within the meaning of this section by reason only that he attends at or near or approaches a dwelling-house or place for the purpose only of obtaining or communicating information. 1953-54, c. 51, s. 52.
- 44. The "prohibited place" subsection was used in England in 1961 in the Chandler case to extend the Act to cases of sabotage. In that case, members of the Committee of 100, a group formed to further the aims of the Campaign for Nuclear Disarmament, were charged with conspiracy to breach the comparable

British "espionage" section by physically disrupting the operation of Wethersfield air base then used by American planes carrying nuclear weapons. They were convicted. Their appeals reached the House of Lords. It was argued that the section was not meant to cover such conduct but was limited to spying. The House of Lords dismissed the appeals of the accused persons from their convictions stating, in the words of Lord Reid, that "it is impossible to suppose that the section does not apply to sabotage and what was intended to be done in this case was a kind of temporary sabotage." In our opinion, in Canada, such conduct should be dealt with under the sabotage section of the Criminal Code, section 52(2)(a), in that the act would impede the "working of any ... aircraft."

WE RECOMMEND THAT the provisions of section 3(1)(a) of the Official Secrets Act relating to a prohibited place be repealed and not be included in new legislation.

[Recommendation 6]

#### B. Harbouring

45. A person may be convicted under the present section 8 of the Official Secrets Act if he has knowledge, or if he has reasonable grounds for supposing, that a person on his premises is about to commit or has committed an offence. The marginal note indicates that this section refers to "harbouring spies" and not to harbouring persons who might merely be guilty of carelessness or leakage of government information. We think that criminal liability for harbouring should only apply in cases in which the accused has knowledge that the person on his premises has committed or is about to commit an espionage offence.

WE RECOMMEND THAT the provisions of section 8 of the Official Secrets Act, the harbouring section, be retained but that the new legislation should make it clear that the provisions would only apply in cases in which the accused has knowledge that the person on his premises has committed or is about to commit an espionage offence.

[Recommendation 7]

#### C. Possession of Espionage Instruments

46. Although it is not now an offence, we think that there should be provision for the prosecution of persons who, without lawful excuse, are found in possession of instruments of espionage such as code books, secret writing materials and microdot equipment. In such a case, the Crown would not be required to prove that any communication or other act of espionage has been committed. The Act now makes it an offence to use false documents of identity in order to obtain admission to a "prohibited place" or for any purpose prejudicial to the safety or interests of the state (section 5). The possession of such false documents could be included in the definition of instruments of espionage and we think that this would be appropriate. The use of such documents, however, can be adequately prosecuted under other provisions of the Criminal Code and we therefore do not think that a similar offence should

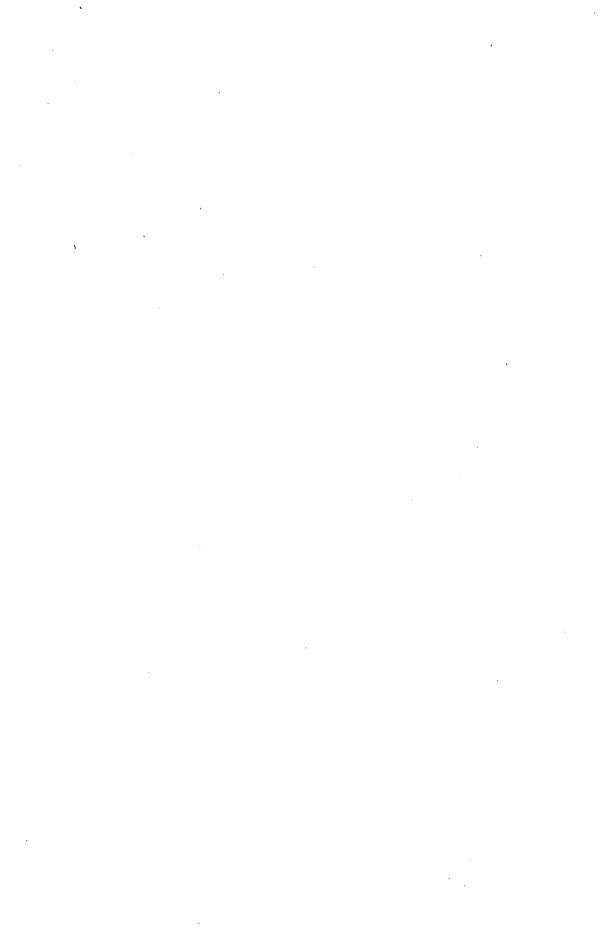
be contained in the legislation relating to espionage. The wording of the offence of possession of instruments of espionage could well follow the language of section 309 of the Criminal Code concerning possession of housebreaking instruments.

WE RECOMMEND THAT the new legislation include the offence of possession of instruments of espionage. Under this provision it would be an offence to be found in possession without lawful excuse of instruments of espionage, which would include false documents of identity.

[Recommendation 8]

#### D. Secret Foreign Agents

- 47. There may be secret foreign agents operating in Canada whose activities may be detrimental to the security of Canada and yet who could not be prosecuted under the espionage laws recommended above. For instance, a secret agent of a foreign power operating over a long period of time may develop a network of contacts who, in the event of war, would be useful to that foreign power. Moreover, there is considerable evidence that in recent years foreign intelligence agencies have changed their emphasis from classical espionage involving theft of a country's secrets to activities designed to develop secret agents of influence within strategic sectors of society, such as government, industry and education. These secret agents may not, for a long period of time, elicit, collect, record or publish information but, nevertheless, their activities may be inimical to Canada's security interests. However, it may be difficult to draw the line between the legitimate "lobbying" activities of a foreign government and the work of an agent of influence.
- 48. This problem might be solved in part by the adoption of legislation which would require all agents of foreign governments to file a detailed registration statement with the government describing the nature of their agency relationship and the extent of the activities performed on behalf of their foreign principals. Those who operate as agents and fail to register would be guilty of an offence. One alternative to the adoption of such legislation would be the enactment of a provision which would make it an offence to be the secret agent of a foreign power. The Commission is considering these questions and will be reporting on them at a later stage.



#### Part VI:

#### LEAKAGE

- **49.** Section 4, the "leakage" section of the Official Secrets Act, imposes criminal sanctions for the improper communication of government information. It provides that:
  - 4. (1) Every person is guilty of an offence under this Act who, having in his possession or control any secret official code word, or pass word, or any sketch, plan, model, article, note, document or information that relates to or is used in a prohibited place or anything in such a place, or that has been made or obtained in contravention of this Act, or that has been entrusted in confidence to him by any person holding office under Her Majesty, or that he has obtained or to which he has had access while subject to the Code of Service Discipline within the meaning of the National Defence Act or owing to his position as a person who holds or has held office under Her Majesty, or as a person who holds or has held a contract made on behalf of Her Majesty, or a contract the performance of which in whole or in part is carried out in a prohibited place, or as a person who is or has been employed under a person who holds or has held such an office or contract,
    - (a) communicates the code word, password, sketch, plan, model, article, note, document or information to any person, other than a person to whom he is authorized to communicate with, or a person to whom it is in the interest of the State his duty to communicate it;
    - (b) uses the information in his possession for the benefit of any foreign power or in any other manner prejudicial to the safety or interests of the State;
    - (c) retains the sketch, plan, model, article, note, or document in his possession or control when he has no right to retain it or when it is contrary to his duty to retain it or fails to comply with all directions issued by lawful authority with regard to the return or disposal thereof; or
    - (d) fails to take reasonable care of, or so conducts himself as to endanger the safety of the sketch, plan, model, article, note, document, secret official code word or pass word or information.
  - (2) Every person is guilty of an offence under this Act who, having in his possession or control any sketch, plan, model, article, note, document or information that relates to munitions of war, communicates it directly or indirectly to any foreign power, or in any other manner prejudicial to the safety or interests of the State.
  - (3) Every person who receives any secret official code word, or pass word, or sketch, plan, model, article, note, document or information, knowing, or having reasonable ground to believe, at the time when he receives it, that the code word, pass word, sketch, plan, model, article, note, document or information is communicated to him in contravention of this Act, is guilty of an offence under this Act, unless he proves that the

communication to him of the code word, pass word, sketch, plan, model, article, note, document or information was contrary to his desire.

- (4) Every person is guilty of an offence under this Act who
- (a) retains for any purpose prejudicial to the safety or interests of the State any official document, whether or not completed or issued for use, when he has no right to retain it, or when it is contrary to his duty to retain it, or fails to comply with any directions issued by any Government department or any person authorized by such department with regard to the return or disposal thereof; or
- (b) allows any other person to have possession of any official document issued for his use alone, or communicates any secret official code word or pass word so issued, or, without lawful authority or excuse, has in his possession any official document or secret official code word or pass word issued for the use of some person other than himself, or on obtaining possession of any official document by finding or otherwise, neglects or fails to restore it to the person or authority by whom or for whose use it was issued, or to a police constable. R.S., c.198, s.4.
- 50. Although the words "secret official" are used in the section, as we have already seen they perhaps qualify only the words "code word" and possibly "password." Thus, it is possible that all government information, whether classified or not, is subject to the section. This is clearly the interpretation given to the comparable section (section 2) of the British Act.
- 51. It will be noted also that the section deals with elements of espionage and with the concept of prejudice to "the safety or interests of the state," which are intermixed with the idea of communication of government information to unauthorized persons. The section prohibits:
  - (i) communication of government information to unauthorized persons. s.4(1)(a)
  - (ii) use of government information for the benefit of a foreign power.s.4(1)(b)
  - (iii) illegal retention of information. s.4(1)(c)
  - (iv) neglect or failure to take reasonable care of such information.s.4(1)(d)
  - (v) communication to a foreign power, of information which relates to munitions of war. s.4(2)
  - (vi) receipt of government information. s.4(3)
  - (vii) retention of information for a purpose prejudicial to the safety or interests of the state. s.4(4)
  - (viii) authorization of the possession of information by other persons. s.4(4)
- 52. The Franks Committee in the United Kingdom, which reported in 1972, stressed the "catch-all" nature of section 2, which is virtually identical to section 4 of the Canadian Act:

The main offence which section 2 creates is the unauthorized communication of official information (including documents) by a Crown servant. The leading characteristic of this offence is its catch-all quality. It catches all official documents and information. It makes no distinctions of kind, and no distinctions of degree. All information which a Crown servant learns in the course of his duty is "official" for the purposes of section 2, whatever its original source. A blanket is thrown over everything; nothing escapes. The section catches all Crown servants as well as all official information. Again, it makes no distinctions according to the nature or importance of a Crown servant's duties. All are covered. Every Minister of the Crown, every civil servant, every member of the Armed Forces, every police officer, performs his duties subject to section 2. (page 14)

53. Similar concerns were voiced in Canada in the debate on the subject in the House of Commons about the broad scope of our section 4. On June 9, 1978, Mark R. MacGuigan, who was at the time chairman of the Standing Committee on Justice and Legal Affairs, said that section 4:

is so sweeping that it is almost difficult to conceive that in strict law any minister or public servant could lawfully communicate any significant information . . .

This is the broadest possible language imaginable. In section 4 the law allows him to communicate only to a person to whom he is authorized to communicate or a person to whom it is in the interest of the state to communicate.

Such a section can have a very chilling effect on the operations of people in government.

(Hansard 1978, page 6251)

- 54. Sir Lionel Heald, a former Attorney General of England, described the breadth of the English section by stating that section 2 "makes it a crime, without any possibility of a defence, to report the number of cups of tea consumed per week in a government department, or the details of a new carpet in the minister's room ... The Act contains no limitation as to materiality, substance, or public interest." (*The Times*, March 20, 1970)
- 55. Whether or not the Attorney General of England was correct in his interpretation of the English section 2, there can be no question but that section 4 of the Canadian Act is too wide in that it imposes criminal liability in many unnecessary situations. Most of these situations could be handled, as they now are, by internal disciplinary action. We believe that criminal penalties should be imposed for the unlawful disclosure of only certain specified types of government information. The 1978 British White Paper, for example, recommended that criminal liability attach to the unauthorized disclosure of government information falling into such categories as defence, internal security, international relations, law and order, confidences of the citizen, and security and intelligence. Cabinet documents and information pertaining to the value of sterling were expressly omitted from this list. Law and order and security and intelligence are the two classes of information with which this Commission is exclusively concerned.
- 56. We believe that it should be an offence to disclose without authorization government information relating to security and intelligence whether or not such information is classified. The British White Paper stated that, "information relating to security and intelligence matters is deserving of the highest protection whether or not it is classified. This is pre-eminently an area where the gradual accumulation of small items of information, apparently trivial in

themselves, could eventually create a risk for the safety of an individual or constitute a serious threat to the interests of the nation as a whole" (page 16). In our view, this observation applies with equal force to Canada.

WE RECOMMEND THAT new legislation with respect to the disclosure of government information should make it an offence to disclose without authorization government information relating to security and intelligence.

[Recommendation 9]

.57. In a prosecution for the unauthorized disclosure of government information relating to security and intelligence the Crown may wish to rely on the security classification of a document in order to show that disclosure was not authorized. In this context, the question arises as to whether, in the course of such a prosecution, a security classification should be considered conclusive or whether a court should be permitted to review the security classification given to a document by the government. In the past, this has not been an issue in Canada or England because all government information, whether classified or not, has been covered by the Act. The Mackenzie Commission recommended that in any new legislation the Minister's designation be conclusive. The Franks Committee also took the position that decisions about classification should be reserved to the government. The Franks Committee did, however, recommend a safeguard which required the appropriate Minister to certify that at the time of the alleged disclosure, as distinct from the time of classification, the information was properly classified. We would recommend a different safeguard. We think that a court should not be bound by the government's classification, even though the judge or jury might be reluctant to disagree with it. If the courts have the responsibility to determine questions relating to the security of Canada in the case of espionage, we fail to see why they should not also have responsibility to review, in the course of a criminal prosecution involving unauthorized disclosure, the appropriateness of the security classification assigned to government information.

WE RECOMMEND THAT the new legislation should empower the court trying an offence of unauthorized disclosure of government information relating to security and intelligence to review the appropriateness of the security classification assigned to such government information.

[Recommendation 10]

58. Also, we believe that it should be a criminal offence to disclose government information of a highly sensitive character which disclosure could adversely affect the administration of criminal justice. In this category, we would include information relating to the investigation of crime, the gathering of intelligence on criminal organizations or individuals and the security of prisons and reform institutions. However, we believe that it should be a defence to a charge of unauthorized disclosure that the accused believed, and had reasonable grounds for believing, that the disclosure of such information was for the public benefit. This defence is consistent with the defences in the Criminal Code in respect of sedition 61(b) and defamatory libel (section 273).

WE RECOMMEND THAT new legislation with respect to the unauthorized disclosure of government information should make it an offence to

'disclose government information relating to the administration of criminal justice the disclosure of which would adversely affect:

- (a) the investigation of criminal offences;
- (b) the gathering of criminal intelligence on criminal organizations or individuals;
- (c) the security of prisons or reform institutions; or might otherwise be helpful in the commission of criminal offences.

  [Recommendation 11]

WE RECOMMEND THAT it should be a defence to such a charge if the accused establishes that he believed, and had reasonable grounds for believing the disclosure of such information was for the public benefit.

[Recommendation 12]

59. Section 4 of the Act permits communication by a person only to someone with whom he is authorized to communicate. If the section were construed so as to require express authorization in every case in which a civil servant discusses government business, then many thousands of offences would be committed every day, particularly with the great increase in consultation that has been taking place at all levels of government. But the courts would undoubtedly interpret the section to permit some form of implied authorization. As the Franks Report stated:

Actual practice within the Government rests heavily on a doctrine of implied authorization, flowing from the nature of each Crown servant's job ... Ministers are, in effect, self-authorizing. They decide for themselves what to reveal. Senior civil servants exercise a considerable degree of personal judgment in deciding what disclosures of official information they may properly make, and to whom. More junior civil servants, and those whose duties do not involve contact with members of the public, may have a very limited discretion, or none at all. (page 14)

Thus, the normal process of consultation, the background briefing or even the government authorized leak, would not contravene the Official Secrets Act. Nevertheless, this aspect of the interpretation of the section is not as free from doubt as it should be and implied authorization should be specifically mentioned in the section. Moreover, we believe that it should be a defence to a charge of unlawful disclosure of government information that even if there was not express or implied authority to disclose, the accused had reasonable grounds to believe and did believe that he was authorized to disclose such information.

WE RECOMMEND THAT the offence of unauthorized disclosure of government information relating to security and intelligence and the administration of criminal justice provide that a person shall not be convicted

- (a) if he had reasonable grounds to believe and did believe that he was authorized to disclose such information, or,
- (b) if he had such authorization, which authorization may be express or implied.

[Recommendation 13]

60. The most controversial part of the leakage provisions of the Official Secrets Act is section 4(3) which directly affects the press. This subsection provides that:

4(3) Every person who receives any secret official code word, or pass word, or sketch, plan, model, article, note, document or information, knowing, or having reasonable ground to believe, at the time when he receives it, that the code word, pass word, sketch, plan, model, article, note, document or information is communicated to him in contravention of this Act, is guilty of an offence under this Act, unless he proves that the communication to him of the code word, pass word, sketch, plan, model, article, note, document or information was contrary to his desire.

There have been many prosecutions in England under the comparable provision. The prosecution against the Toronto Sun was the first such prosecution against a newspaper in Canada. The British White Paper (page 17) proposes that the "mere receipt of protected information" by those who are neither Crown servants nor government contractors should not be a criminal offence, but that communication by the recipient should be. This will not satisfy those who wish to be able to print unlawfully leaked information without fear of prosecution. Nevertheless, in the case of government information relating to security and intelligence or the administration of criminal justice, positive harm would result in most cases if the information were published. Consequently, we agree with the British position that communication of such information by the recipient be a criminal offence.

WE RECOMMEND THAT the communication of government information relating to security and intelligence or the administration of criminal justice by a person who receives such information, even though such information is unsolicited, be an offence.

[Recommendation 14]

- 61. Section 4 also makes the following "passive" acts offences:
  - (i) illegal retention of documents when a person has no right to retain them or when it is contrary to his duty to retain them. s.4(1)(c)
  - (ii) retention of documents for any purpose prejudicial to the safety or interests of the state. s.4(4)
  - (iii) failure to take reasonable care of documents or information. s.4(1)(d)

We agree with the intent of section 4(1)(c) that the retention of certain government information be an offence. The section should be drafted in such a way, however, so as to make it clear that there is a duty to return such documents to an authorized person as soon as possible and without any demand from the government. In other words, we feel that all citizens, including members of the press, are under a public duty to return documents relating to security and intelligence or to the administration of criminal justice should such documents come into their hands.

WE RECOMMEND THAT it be an offence to retain government documents relating to security and intelligence or to the administration of criminal justice notwithstanding that such documents have come into the possession of a person unsolicited and that there has been no request for the return of such documents.

[Recommendation 15]

62. We do not agree, however, that criminal liability should attach to the negligence of a civil servant or a government contractor who fails to take

reasonable care of secret government information unless such conduct shows wanton or reckless disregard for the lives or safety of other persons or their property. In other circumstances, the appropriate means of discouraging such negligence are vigilant administration and disciplinary action.

WE RECOMMEND THAT the failure to take reasonable care of government information relating to security and intelligence or to the administration of criminal justice not be an offence unless such conduct shows wanton or reckless disregard for the lives or property of other persons.

[Recommendation 16]

### Part VII:

### SOME GENERAL ISSUES

63. We now propose to turn our attention to some general issues under the Official Secrets Act which relate to both espionage and leakage.

### A. Attorney General's Fiat

64. Section 12 of the Official Secrets Act requires that the Attorney General of Canada give his personal consent to the institution of all prosecutions under the Act. The section does not appear to apply to a charge of conspiring to breach the Act since such charges are brought pursuant to the Criminal Code. Because questions of national security are involved, as well as, in many cases, international relations, we think that the decision to prosecute, whether it is for the offence of espionage, or for conspiracy to commit such offences, or for the unauthorized disclosure of that federal government information discussed in this report should be made by the Attorney General of Canada. For the same reasons, it is our view that the conduct of such prosecutions should be the responsibility of the Attorney General of Canada.

WE RECOMMEND THAT the consent of the Attorney General of Canada be required for the prosecution of espionage offences, conspiracy to commit espionage offences, or offences relating to the unauthorized disclosure of that federal government information discussed in this report. Similarly, the conduct of such prosecutions should be the responsibility of the Attorney General of Canada.

[Recommendation 17]

#### B. In Camera Trials

65. It is a fundamental principle of our democratic system that trials should be conducted in public and not in secret. Even espionage trials which concern the security of the state should not be held completely in camera. The Official Secrets Act does not contemplate a hearing completely in camera. Instead, it envisages the commencement of proceedings in public and specifically requires that sentencing take place in public. Section 14(2) of the Act provides that "the passing of sentence shall in any case take place in public" but that the court may make an order that "all or any portion of the public shall be excluded during any part of the hearing," if, "in the course of proceedings ... application is made ... that the publication of any evidence to be given or of any statement to be made in the course of the proceedings would be prejudicial to the interests of the State." By way of contrast, the American constitution requires a fully "public" trial. This has resulted in the prosecution

having to choose between publicly disclosing information which would be prejudicial to the interest of the state and the alternative of running the risk of having the prosecution dismissed if it fails to disclose the information.

- 66. While section 2(f) of the Canadian Bill of Rights states that an accused must be "proven guilty according to law in a fair and *public* hearing by an independent and impartial tribunal," we should not assume that this provision will influence the interpretation of the specific words of section 14(2) of the Official Secrets Act.
- 67. As we have noted, the *in camera* hearing in the *Treu* case gave rise to considerable controversy. The application for the *in camera* hearing was made, to quote the Hon. Otto Lang speaking on behalf of the Minister of Justice, "because the documents which would be reviewed included a large number of NATO documents and testimony of witnesses concerning those documents" (Hansard 1978 page 6243). Although the accused's counsel did not formally consent to a closed hearing, neither did he make any objection. Moreover, when Treu's convictions were quashed by the Quebec Court of Appeal, no criticism was made of the *in camera* procedure. In fact, Kaufman, J.A., was of the view that the trial judge "faced with an application for the exclusion of the public had little choice but to grant this since, at the outset, he could hardly foresee the nature of the case and the importance of each piece of evidence. His discretion was therefore severely restricted, and no blame should be attached to his decision to proceed *in camera*. It was, at the time, the only safe course to adopt."
- 67A. The Toronto Sun case, which was not held in camera, points out the difficulties which can be experienced by the prosecution in handling confidential documents and evidence. At an early stage of the preliminary inquiry, the defence was given access to the Security Service files by the Crown and subsequently the defence asked the judge to issue a subpoena to compel production of R.C.M.P. files. This turn of events was a cause of embarrassment to the Security Service. After extensive consultations had taken place in Ottawa and the documents had been reviewed by the Solicitor General, it was decided to rely on Section 41 of the Federal Court Act and refuse to produce the files. The affidavits of the Solicitor General which were filed in Court under Section 41 stated that more than 17,000 documents could not be produced, but that the majority of these documents could be made available to the trial judge who could then determine whether they were appropriate for release. After the Court had made a preliminary examination of the documents, the Crown changed its position and indicated that the prosecution would proceed without relying on the documents at all. This case illustrates the importance of adequate consultation before the trial, and indeed where possible before the charges are laid, among the Security Service, the Solicitor General and the Attorney General of Canada.
- 68. In our view, it would be in the public interest to have all espionage trials conducted in public to the greatest extent possible, notwithstanding the consent of the accused to have the entire proceedings in camera. This will require the

presiding judge to hold in camera only those parts of the trial that must be kept confidential for reasons of national security.

- 69. For these reasons, a pre-trial proceeding in camera might in some cases reduce or even eliminate the need for an in camera trial. Such a proceeding could be used in cases in which secret information is likely to be disclosed in the course of the prosecution. The judge would be required to rule in advance of the trial as to the admissibility in public of any intelligence information and as to the manner in which the testimony of intelligence community witnesses would be received. In Featherstone, for example, the judge consented to witnesses from the Security Service testifying anonymously in camera on condition that the testimony, without attribution, would later be released to the press.
- 70. The legislation should make it clear that the words "any part of the hearing" in s.14(2) may not be construed so as to permit the exclusion of the public for the entirety of the trial except in rare circumstances in which public disclosure of every part of the evidence would constitute a threat to national security. Once this is made clear, the prosecution could not, even with the consent or non-objection of the defence, follow the course of asking for a completely in camera trial. The prosecution would have to ask for the exclusion of the public at that point of the trial when it became necessary to lead sensitive evidence or became necessary to ask the witnesses for the defence questions the answers to which would be sensitive.
- 71. We therefore are of the view that section 14(2) permitting in camera proceedings be retained in respect of espionage offences and in respect of unlawful disclosure of those categories of government information discussed above. Section 14(2) should be amended, however, so that the phrase "prejudicial to the interest of the State" will read "prejudicial to the security of Canada or to the proper administration of criminal justice." Finally, in order to emphasize the duty of the trial judge to hold as much of the trial as possible in public, the last clause of section 14(2) might read "but except for the foregoing, the trial proceedings, including the passing of sentence, shall take place in public." The section should also provide for an in camera pre-trial procedure as indicated above.

WE RECOMMEND with respect to s.14(2) of the Official Secrets Act which permits "in camera" proceedings that:

- (a) the provisions of section 14(2) be retained and made applicable to all offences, either offences in new legislation or in the Criminal Code, in which the Crown may be required to adduce evidence the disclosure of which would be prejudicial to the security of Canada or to the proper administration of criminal justice.
- (b) the phrase "prejudicial to the interest of the state" read "prejudicial to the security of Canada or to the proper administration of criminal justice."
- (c) the last clause of the section read "but except for the foregoing, the trial proceedings, including the passing of sentence, shall take place in public."

(d) the legislation make provision for the holding of an in camera pre-trial conference for the purpose of dealing with procedural questions relating to the handling of evidence which might have to be received in camera.

[Recommendation 18]

### C. Procedure for Trying the Cases

72. All offences in the Official Secrets Act can be tried either summarily or by indictment. This is at the option of the Crown whose election cannot be challenged by the accused. If the Crown proceeds summarily, the possible maximum penalty is twelve months or a fine of five hundred dollars or both; if by indictment, the maximum penalty is fourteen years. The 1920 British Official Secrets Act also permits a summary trial, but this does not apply to the espionage section. Perhaps nowhere else in Canadian criminal law is there such a wide discrepancy between the penalty for the indictable offence and the penalty for the summary offence. Furthermore, nowhere else in Canadian criminal law can an accused be deprived of a jury for such a serious offence or one with such important political overtones. In the case of espionage offences and leakage offences relating to security and intelligence and the administration of criminal justice, we do not feel that the summary conviction procedure should be retained.

WE RECOMMEND THAT offences dealing with espionage and the unauthorized disclosure of information relating to security and intelligence and the administration of criminal justice should be required to be tried by indictment and not by summary conviction.

[Recommendation 19]

- 73. One aspect of trial by jury which has recently been the subject of controversy in the United Kingdom is the "vetting" of the jury panel in advance of the case. In the ABC case, a list of jurors was obtained by an ex parte application to a judge to enable the prosecution to check the jury panel for "disloyal" members. (Sunday Times, Oct. 1, 1978) In Canada, the names, addresses and the occupations of the members of the jury panel are usually available to the prosecution and the defence in advance of the trial. Furthermore, the Crown in Canada has a very wide right to ask jurors to "stand aside," which can be used to weed out jurors who might be regarded as potential security risks.
- 74. While we believe that the Crown should be permitted to conduct security checks on prospective jurors, we do not think that the Crown should have any greater right than the defence to obtain a list of jurors in advance of the trial. If such a list is obtained, then both sides should be able to make whatever inquiries are permitted in any criminal case.

WE RECOMMEND THAT the Crown have no special right to "vet" a jury in security cases over and above the rights now provided in the Criminal Code and under provincial law.

[Recommendation 20]

75. It is not clear whether jurors who hear evidence in camera are governed by the existing leakage provisions of the Official Secrets Act. Presumably they are. In our opinion, the legislation should specifically provide that jurors are subject to the leakage provisions.

WE RECOMMEND THAT new legislation provide that jurors who participate in proceedings in camera be subject to the offences relating to the unauthorized disclosure of government information.

[Recommendation 21]

### D. Penalties

- 76. The penalties imposed by the Act need to be reassessed. In our opinion, the penalty for espionage may be too low whereas the penalty for leakage is clearly too high.
- 77. The penalty for espionage is now a maximum of fourteen years, having been raised in 1950 from seven years. Espionage is an extremely serious offence. Its extraordinary gravity in certain circumstances is illustrated by the fact that the English courts have imposed extremely long sentences (Blake in 1961 received 42 years) by resorting to the imposition of cumulative sentences on multiple counts. We consider the maximum sentence for espionage should be life imprisonment to be imposed in the discretion of the trial judge in appropriate cases. On the other hand, as noted above, if the information communicated to a foreign power is information accessible to the public then the penalty should be less.

WE RECOMMEND THAT the maximum penalty for espionage be life imprisonment, except in the case of the communication to a foreign power of information accessible to the public in which case the maximum penalty should be six years.

[Recommendation 22]

78. The fourteen year penalty is surely inappropriate for leakage cases. The maximum penalty in Britain is now only two years. In our opinion, the penalty should be more in line with section 111 of the Criminal Code, dealing with breach of trust by a public officer, which carries a maximum penalty of six years.

WE RECOMMEND THAT the maximum penalty in a case of unauthorized disclosure of government information relating to security and intelligence or the administration of criminal justice, be six years.

[Recommendation 23]

### E. Presumptions and Attempts

79. The Act's "unusual evidential and procedural provisions" appeared to the Mackenzie Commission to be "extraordinarily onerous." (page 23) There is no doubt that the extent of the evidentiary provisions in section 3 of the Official Secrets Act is unusual and probably unnecessary. Some of the provisions were introduced in 1911 to make it easier for the Crown to prove that the accused's purpose was prejudicial to the interests of the state. Further and stronger

evidentiary provisions were added in the 1920 legislation. The relevant parts of section 3 read as follows:

- 3. (2) On a prosecution under this section, it is not necessary to show that the accused person was guilty of any particular act tending to show a purpose prejudicial to the safety or interests of the State, and, notwith-standing that no such act is proved against him, he may be convicted if, from the circumstances of the case, or his conduct, or his known character as proved, it appears that his purpose was a purpose prejudicial to the safety or interests of the State; and if any sketch, plan, model, article, note, document or information relating to or used in any prohibited place or anything in such a place, or any secret official code word or pass word is made, obtained, collected, recorded, published or communicated by any person other than a person acting under lawful authority, it shall be deemed to have been made, obtained, collected, recorded, published or communicated for a purpose prejudicial to the safety or interests of the State unless the contrary is proved.
- (3) In any proceedings against a person for an offence under this section, the fact that he has been in communication with, or attempted to communicate with, an agent of a foreign power, whether within or outside Canada, is evidence that he has, for a purpose prejudicial to the safety or interests of the State, obtained or attempted to obtain information that is calculated to be or might be or is intended to be directly or indirectly useful to a foreign power.
- (4) For the purpose of this section, but without prejudice to the generality of the foregoing provision
  - (a) a person shall, unless he proves the contrary, be deemed to have been in communication with an agent of a foreign power if
    - (i) he has, either within or outside Canada, visited the address of an agent of a foreign power or consorted or associated with such agent, or
    - (ii) either within or outside Canada, the name or address of, or any other information regarding such an agent has been found in his possession, or has been supplied by him to any other person, or has been obtained by him from any other person.
  - (b) "an agent of a foreign power" includes any person who is or has been or is reasonably suspected of being or having been employed by a foreign power either directly or indirectly for the purpose of committing an act, either within or outside Canada, prejudicial to the safety or interests of the State, or who has or is reasonably suspected of having, either within or outside Canada, committed, or attempted to commit, such an act in the interests of a foreign power; and
  - (c) any address, whether within or outside Canada, reasonably suspected of being an address used for the receipt of communications intended for an agent of a foreign power, or any address at which he resorts for the purpose of giving or receiving communications, or at which he carries on any business, shall be deemed to be the address of an agent of a foreign power, and communications addressed to such an address to be communications with such an agent.

- 80. Section 3(2) of the Act makes it easier for the Crown in a variety of ways. In the first place, it states that "it is not necessary to show that the accused person was guilty of any particular act tending to show a purpose prejudicial to the safety or interests of the State." This makes clear what would probably have been the interpretation in any case. The section also says that the accused "may be convicted if, from the circumstances of the case, or his conduct, or his known character as proved it appears that his purpose was a purpose prejudicial to the safety or interests of the State." This provision changes the law because it allows as evidence material concerning the accused's character which would not normally be permitted as evidence-inchief in a criminal case, and because it allows the introduction of similar fact evidence which is not usually permitted. Finally, the section provides that, if any information relating to a prohibited place is unlawfully communicated, "it shall be deemed to have been ... communicated for a purpose prejudicial to the safety or interests of the State unless the contrary is proved," thus shifting the onus of proof from the Crown to the accused person. It is interesting to note that the American Justice Department had proposed legislation in their 1911 Espionage Act modelled on this section of the British Act, but it was eliminated by the House Judiciary Committee on the ground that it was regarded as "not fair."
- 81. Section 3(3) provides that the fact of an accused's communication with a foreign agent "is evidence that he has, for a purpose prejudicial to the safety or interests of the State, obtained or attempted to obtain information that ... might be ... useful to a foreign power." Section 3(4) provides that a person "shall, unless he proves the contrary, be deemed to have been in communication with an agent of a foreign power" if he has visited the address of the agent or associated with the agent or the name or address of the agent is found in his possession. "Agent" is defined to include any person who is "reasonably suspected" of being employed by a foreign power for the purpose of committing an act prejudicial to the safety or interests of the state.
- 82. These provisions would appear to us to be unnecessary. Convictions can surely be obtained in serious espionage cases without them. This was the view of one of the principal prosecutors in the Gouzenko trials, John Cartwright, later the Chief Justice of Canada, who stated that he did not "think that any of those who were convicted were convicted because of any special statutory presumptions which the Act contains." (quoted in Hansard 1950, page 4013) In our opinion, the Crown does not require the assistance of these unusual presumptions, especially having regard to the normal inferences that a judge and jury can draw from circumstantial evidence.

WE RECOMMEND THAT the presumptions in favour of the Crown in section 3 of the Official Secrets Act not be incorporated in the new legislation.

[Recommendation 24]

- 83. Section 9 of the Act establishes the following as offences:
  - (1) an attempt to commit any offence under the Act
  - (2) the soliciting, inciting or persuading of another person to commit an offence

- (3) the aiding and abetting the commission of an offence, and,
- (4) the doing of any act preparatory to an offence.

Although we agree with the general purpose of this section, we do not feel that there is any justification for an offence of doing of "any act preparatory to the commission of an offence." Making an offence of an act of mere preparation, as distinct from conspiring to commit an offence, is beyond the normal scope of the criminal law (although comparable language is used in the Code in relation to the extremely grave offence of high treason, s.46(2)(d)). We therefore recommend that the offence of preparatory acts be repealed.

WE RECOMMEND THAT the offence of doing an act preparatory to the commission of an offence under the Official Secrets Act be removed but that the other offences found in section 9 be retained in the new legislation and made applicable to the offences of espionage and the unauthorized disclosure of government information relating to security and intelligence and the administration of criminal justice.

[Recommendation 25]

### F. The Applicability of the Law

84. The espionage and leakage laws apply to all persons who commit an offence within Canada. Where such conduct occurs abroad, the Official Secrets Act applies to those persons who were Canadian citizens at the time of the commission of the offence (section 13(a)) or who owed allegiance to the Crown at the time the document or information was obtained (section 13(b)). In our opinion, these provisions should continue to apply to espionage offences and to leakage offences relating to security and intelligence. This permits prosecution in broader circumstances than those provided under section 46(3) of the Criminal Code relating to treason, which appears to allow a defector from Canada to avoid a treason charge if he communicates secrets after he leaves Canada and after he has renounced his citizenship. We believe that such a person should not be able to escape a conviction under the Official Secrets Act should he return to Canada.

WE RECOMMEND THAT the provisions of sections 13(a) and 13(b) of the Official Secrets. Act which make the Act applicable to offences committed abroad be retained in the new legislation.

[Recommendation 26]

85. It should be noted that the Official Secrets Act is also applicable to the disclosure of provincial information because section 4 applies to information obtained "owing to his position as a person who holds or has held office under Her Majesty" and that the latter phrase is defined by section 2 to include "any office or employment in or under any department or branch of the government of Canada or of any province . . . ." There have been no reported cases relating to the disclosure of provincial information.

#### G. Location of the Provisions

86. In order to effect our recommendations, we feel that the Official Secrets Act should be repealed and replaced with new legislation. This legislation in so

far as it relates to espionage could take the form of a new act or an equally acceptable solution would be to place all national security offences in one part of the Criminal Code.

WE RECOMMEND THAT the Official Secrets Act be repealed and replaced with new legislation with respect to espionage, which should be incorporated in a new statute or placed in one part of the Criminal Code with all other national security offences.

[Recommendation 27]

87. As we have stated above, espionage is quite distinct from the leakage of government information and therefore offences relating to leakage should be clearly separated from national security offences either in a separate statute dealing with government information or in a different part of the Criminal Code.

WE RECOMMEND THAT the legislative provisions with respect to the unauthorized disclosure of information relating to security and intelligence and the administration of criminal justice be clearly separated from the legislative provisions with respect to espionage.

[Recommendation 28]

•

•

.

•

#### FREEDOM OF INFORMATION

### Introduction

- 88. We turn now to another aspect of security and information, viz., freedom of information legislation. It will be recalled that, unlike the "leakage" provisions canvassed above, freedom of information legislation affords a general public right of access to government information, and not a prohibition against its disclosure. Such a statutory right of access is invariably qualified by the exemption of certain classes of documents from disclosure, such as cabinet minutes and national defence matters.
- 89. Our terms of reference do not allow us to make any comments on the merits or demerits of freedom of information legislation per se. However, we do believe that it is within our mandate to make recommendations as to how such legislation should apply to security and intelligence activities and the administration of criminal justice. Consonant with the principle of openness in government, there is a considerable body of information relating to security and intelligence activities which can and should be made public. Such things as the mandates (role and functions) of the security agencies, the general controls regulating their activities (permissible powers of investigation) and the manner of their accountability should be debated in public and the government's position should be made known. But there are areas of the government's security and intelligence activities which cannot be made public without completely destroying their effectiveness. Similarly, there are areas of the administration of criminal justice as to which the disclosure of information would cause grave damage to the criminal justice system.
- Underlying the principle of openness in government is the assumption that such openness will aid in making the government more accountable to the governed. In the fields of security and intelligence and the administration of criminal justice we believe that there is considerable scope for openness but on the other hand there are a number of specific types of information which should remain secret. We appreciate that there are two ways of approaching freedom of information legislation. The general principle can be either that all government information is to be accessible to the public except for certain specified information which is to remain secret, or that all government information is to remain secret except for certain specified information which is to be made public. Similar principles can be applied to any particular category of government information as, for example, security and intelligence. We do not feel that it is necessary or appropriate for us to decide what the general principle should be. In this report we have set out certain categories of security and intelligence information that we think should be made public and we have recommended categories of security and intelligence information and

administration of criminal justice information that we feel should remain secret. In describing those categories in this report we have referred to them as exemptions: this has been done on the assumption that Parliament will opt for the general principle that openness should be the rule and secrecy the exception. We wish to emphasize that in those areas where non-disclosure is to prevail methods of accountability can and should be implemented which will serve as a satisfactory substitute for public disclosure, and will also protect individuals aggrieved by the security apparatus of government or the criminal justice system.

91. A related matter to be examined is whether, in judicial proceedings, there should be statutory provisions limiting disclosure of evidence concerning questions of security and intelligence, and the nature of any such provisions.

### Part I:

# PROTECTION OF SECURITY AND INTELLIGENCE INFORMATION FROM DISCLOSURE UNDER FREEDOM OF INFORMATION LEGISLATION

### A. The Competing Interests

- 92. There are a number of competing interests which must be balanced in determining how much security and intelligence information ought to be protected from disclosure. There are two main interests which weigh in favour of relaxing the strictures on disclosure of such information. First, there is the public's interest in the scrutiny and control of all arms of government, including the security activities. A broader public consciousness of security agencies' operations, generated by greater freedom of information, might go some distance in satisfying this interest. Also militating in favour of greater openness is the right of a citizen to some recourse if he believes he has unjustifiably been adversely affected by the security machinery of government (e.g., failure to obtain a security clearance).
- 93. The reason for greater secrecy, on the other hand, is simple but weighty: if the government is to function effectively in the security and intelligence field, then most, although not all, of its operations and activities must remain secret. If the operational and investigative techniques and structures are revealed and the extent of resources and capabilities is known, the effectiveness of the activities is being undermined. It is essential to bear in mind that serious threats to the security of Canada are posed by foreign intelligence agencies and terrorist groups. These organizations are highly secretive and have developed sophisticated and well financed techniques for obtaining information about the counter-intelligence operations directed against them. A right of access to the operational or organization files relating to security and intelligence would virtually destroy the government's capacity for maintaining surveillance of foreign intelligence agencies and terrorist groups operating in Canada.
- 94. In balancing the interests which are involved we feel that much more information with respect to security and intelligence can be made available than has been the case in the past. All of the general authority granted to the government's security and intelligence agencies (the definition of their role and functions), all the general controls imposed on those activities (their permissible powers of investigation) and the manner of their accountability can and should be the subject of public knowledge and debate. However, we believe that virtually all operational and administrative security and intelligence

information must be exempt from disclosure under freedom of information legislation. The following factors lead us to this latter conclusion.

- (a) Penetration is one of the principal modes of operation of hostile intelligence agencies. Such penetration is assisted immeasurably by the use by hostile agencies of operational and administrative information obtained under freedom of information legislation, unless adequate exemptions are provided.
- (b) Security and intelligence activities cannot be carried out effectively without the use of informants. Informants are the main source of information for security and intelligence agencies. Whether the informants are paid or voluntary they invariably provide the information on the basis that their identity will be kept secret and that every effort will be made to ensure that it remains so. Their reasons for wanting their identity to remain secret are myriad and include fear of physical retaliation, harassment or ostracism. Any uncertainty about the ability of agencies to keep sources confidential will result in a "drying up" of such sources.
- (c) Information provided by foreign governments and foreign intelligence agencies is usually given on the express undertaking that it will not be disclosed to anyone outside of the agency to which it is provided. If confidentiality cannot be guaranteed for this information it too will "dry up".
- (d) Disclosure of the identities of organizations and individuals which are the targets of the security and intelligence agencies or the methodology used in the "targetting" would permit the targets to take action to thwart the investigations of the agencies.
- (e) There are alternative means of satisfying the competing interests mentioned above.

We gain additional comfort in our conclusion by the lessons drawn from a comparative study of freedom of information legislation in other western democracies, which we discuss below.

- 95. Let us first examine what alternative measures would satisfy the societal interests which are at stake in determining the extent of freedom of information legislation exemptions. There are a number of ways of ensuring informed democratic scrutiny and control over government security and intelligence activities besides legislation providing for disclosure of information. For example, there might be rigorous scrutiny mechanisms, subject to democratic control, which could review and survey such activities as well as make public enough information to satisfy the electorate that:
  - (i) the security needs of the country are being met; and
  - (ii) the conduct of the security and intelligence agencies is acceptable.

As for the desirability of an individual citizen having assurance that confidential government information concerning him is accurate and is not being misused, there are certainly alternatives to his having immediate recourse to the government's security and intelligence files. There might be a board of review or appeal which could investigate and adjudicate upon the case of the individual who has been refused a security clearance, or even of an individual who suspects that he is being monitored or interfered with by the government's security and intelligence activities. It is more difficult, indeed impossible to

find alternatives to secrecy as a condition for the effective operation of the government's security and intelligence activities. The more that is revealed about the government's capabilities, priorities and techniques, the easier it will be for hostile agencies and "targetted" organizations and individuals to counter its efforts.

- 96. Thus, while the interests of an informed electorate and of fair treatment of citizens by the security apparatus of government may be met otherwise than by opening the government's security and intelligence files to the public, there are no practical alternatives to the requirement of secrecy as a condition of the effective functioning of that security apparatus.
- It should also be pointed out that allowing public access to most security and intelligence files would not really promote the interest of democratic control over the security agencies, and would not offer much protection to the individual with "security" problems. For as a means of monitoring security and intelligence activities, freedom of information legislation is at best a haphazard way of "spot-checking" those activities. The capacity of freedom of information legislation to attain this goal would depend on the chance that the files requested are those which would reveal undesirable or improper activity, and that the right requests for general information are made. Further, there is no guarantee that truly important information will be released, such as a document indicating a breakdown in the chain of authority. The function of scrutinizing the operations of a security or intelligence agency should be systematic and continual. It is a sensitive and important task, which must be performed assiduously by highly competent people who are also responsible to democratically elected representatives. A freedom of information law, as an aid to the public in policing security and intelligence activities, is of dubious effectiveness. In the case of the individual who believes he has been wronged by a security or intelligence agency, the simple knowledge of what information the government has on him is not in itself enough: he must be allowed to state his case and he must have a remedy. This right to be heard and to obtain redress may be possible without his having access to security and intelligence files.
- 98. Support for our view is found in the experience of some other western democracies. Seven foreign states have been surveyed; the United States, Great Britain, Australia, Sweden, Norway, Finland and Holland. Britain does not have any freedom of information legislation. Sweden, despite its deserved reputation for open government and its constitutionally entrenched freedom of information law, has framed its statutory exemptions broadly enough to cover comfortably the activities of its security and intelligence service. Such is also the case with Norway and Finland, which have broad security exemptions. The freedom of information proposals in the Netherlands and Australia would clearly exempt security and intelligence agency files. The difficulties encountered by U.S. security and intelligence and law enforcement agencies which have arisen as a result of loosely drafted security exemptions have been fairly well documented. The main problems faced by these agencies are the disclosure of certain information from investigative files, the release of material which sheds light on investigative techniques and procedures, and the revelation of

information which is helpful in the identification of confidential sources. These problems are serious ones, and serve to alert us to the dangers of incomplete protection of the government's security and intelligence files from a public right of access.

## B. Protecting those Interests Affected by Non-Disclosure of Security and Intelligence Information

- 99. It is important that we add one qualification to our position against disclosure of certain security and intelligence information. The adoption of such an approach to security and intelligence exemptions must be conditional on the early establishment of measures which will satisfy the need for informed democratic control over the security agencies, and which will protect the rights of individual citizens who feel aggrieved by the security machinery of government.
- 100. We are committed in principle to the establishment of new, more effective, democratically responsible mechanisms and procedures to oversee and control the government's security activities. There are several forms of scrutiny and control mechanisms which we are considering. We are still developing our proposals in this regard, and will make our recommendations in detail in a later report. One method of control to which we are firmly committed is that each security agency should be required to disclose to the appropriate Attorney General any evidence in that agency's records of illegal or improper conduct by members of the agency. We are examining the mechanisms whereby that may be achieved.
- 101. Throughout this Report we refer to the government's "security and intelligence activities" and to "security and intelligence agencies". These phrases require more precise definition. At the present time there is little public knowledge of the responsibilities of various components of the "security and intelligence community", aside from the 1975 Cabinet Directive to the R.C.M.P. Security Service. A prime responsibility of our Commission is to make recommendations to the government of Canada as to the form and content of the mandate which should govern the security service's activities in the future. This we shall do in a later report. Unless the mandates of the other agencies of government responsible for security and intelligence are also clearly spelled out in some public form, there will be great uncertainty about the application of the exemptions we are recommending. Those responsible for applying and reviewing the application of the exemptions will otherwise lack any clear guide as to which agencies' files are to be protected. Therefore, in our view, the government, in order to ensure proper administration of the exemptions, should publish, so far as possible, the terms of reference of all agencies of government carrying out security and intelligence activities.

### C. Specific Security and Intelligence Information that should be Protected

- 102. What specific types of information pertaining to the government's security and intelligence activities need protection? We find that the main classes of such information are:
  - 1. operations files
  - 2. intelligence information files
  - 3. information obtained from confidential sources
  - 4. policy papers and intelligence analyses
  - 5. manuals and directives of security and intelligence agencies
  - management, personnel and financial information, of security and intelligence agencies
  - 7. resources information with respect to security and intelligence agencies
  - 8. information received in confidence from foreign governments and security and intelligence agencies
  - 9. structures of security and intelligence agencies
  - 10. intra-governmental structural relationships respecting security and intelligence
  - 11. inter-governmental structural relationships respecting security and intelligence

These classes should be explained briefly.

- 103. Operations files would include records of past and present security and intelligence investigations and operations. The need for secrecy with regard to what the security and intelligence agencies are doing, and what they have done, seems clear. Disclosure of such information would assist hostile agencies and "targetted" organizations and individuals in their attempts to neutralize Canadian security and intelligence operations.
- 104. Intelligence information files would comprise both highly sensitive information and apparently innocuous pieces of knowledge (e.g., newspaper clippings). The release of either type of information would assist hostile agencies and "targetted" organizations and individuals in divining what our security agencies know, what they do not know, and, in the case of newspaper clippings and other "low sensitivity" information, what specific matters the agencies are interested in.
- 105. Information obtained on the basis that the source will remain confidential would include information from individual informants which, if released, might reveal their identities. Also protected should be information obtained from other Canadian security and intelligence organizations, law enforcement agencies, and public institutions such as hospitals and universities. Release of such information would quickly discourage informants, be they individuals, agencies, organizations or institutions, from entrusting confidential information to the security agencies.
- 106. Policy papers and security analyses would include documents relating to the role and operations of the security and intelligence agencies, as well as perceived security threats. Release of such information would enable hostile

agencies to chart the direction and plans of our security and intelligence agencies.

- 107. Security and intelligence agencies' manuals and directives would include internal documents comprising operational, procedural and technical instructions to security and intelligence agencies' members. Disclosure of such information would reveal to hostile agencies, in precise detail, how the security or intelligence agency operates.
- 108. Management, personnel and financial information would relate to documents concerning the command structures of the security and intelligence agencies, their personnel policies and practices and their planning and management systems. It would also include any details of the financing of the agencies but would not include general information about the overall costs of the government's security and intelligence activities. Release of any detailed information would assist hostile agencies in their efforts to penetrate the security and intelligence agencies.
- 109. Resources information would include documents relating to human, physical and technical resources of the security and intelligence agencies. Disclosure of this information would reveal to hostile agencies the capabilities and limitations of our security and intelligence agencies.
- 110. Information received in confidence from foreign governments and security and intelligence agencies comprises a large part of the information of Canadian government security and intelligence agencies. Virtually all of that information is delivered to our agencies on the distinct understanding that it will not be disclosed without the express prior consent of the supplier. Unless such understandings are honoured the foreign governments and agencies will cease to supply the information, which would have a crippling effect on our agencies' effectiveness.
- 111. Information concerning the structures of our individual security and intelligence agencies and the intra-governmental and inter-governmental structures in which they operate would serve as invaluable data in the hands of hostile security agencies, both for purposes of penetration and for thwarting the activities of our security and intelligence agencies. Such information is indispensable to a hostile agency if it is to fully understand the operations of our security and intelligence agencies.

### D. The Method of Protection of Security and Intelligence Information

112. The drafting of security and intelligence exemptions in freedom of information legislation is extremely complex. Indeed, the question of how the information is protected is as important as the initial decision as to what should be protected. While we do not intend to assume the role of the legislative draftsman, we have some comments on how certain security and intelligence leakage problems may be avoided by certain drafting techniques.

113. First, we believe there should be a special exemption for security and intelligence documents. "Law enforcement", "national defence" and "foreign relations" extend to only part of security and intelligence agencies' activities. They do not cover, for example, the collection and dissemination of domestic intelligence which has for its end something other than law enforcement proceedings, as, for example, security clearance investigations. Nor is it realistic to describe much of the work of investigating activities of foreign intelligence agents as "law enforcement" or "national defence". Frequently the reason the activities of such groups or persons are of concern is not because there is an imminent danger that they will break the law or because their activities will lead to an invasion in the foreseeable future. The extreme sensitivity of this area of government operations requires that such an exemption be heavily weighted in favour of secrecy, more so than is required for matters such as trade secrets and internal working papers of departments.

### WE RECOMMEND THAT there be a specific exemption from disclosure in freedom of information legislation for certain security and intelligence documents.

[Recommendation 29]

114. Second, the security and intelligence exemption should be framed so that it covers not only documents in the files of the security and intelligence agencies, but also information in any other government departments, such as the Department of the Solicitor General and the Privy Council Office, which relates to the security and intelligence subject matters discussed above.

### WE RECOMMEND THAT the exemption for security and intelligence documents extend to all departments and agencies of the government.

[Recommendation 30]

Third, the statutory test used to determine whether a request for information may be granted should be one which refers to the nature, or subject-matter, of the document requested. It should not be a test which requires the assessment of possible or probable harm to a specified interest which might be suffered if the material in question is disclosed. The disadvantage of such a "damage to interest" test is in the difficulty of its application to highly sensitive material such as security and intelligence information. The task of forecasting accurately damage which may be incurred by the release of security information is impossible. Especially when this test is coupled with a "severability" requirement (i.e., that if only a portion of the record is sensitive, then only that part is to be retained and the rest of the record released), the judgment whether the release of certain parts of the document would or could harm the specified interest becomes an exceedingly delicate and complex decision. It is easy even for a skilled intelligence analyst to make a mistake, especially in a case where it is a question of deciding whether the disclosure of certain facts might help a target identify a confidential source. Moreover, in security and intelligence as in no other area of government information gathering, such a test would impose a real difficulty upon the government's security and intelligence agencies. Security intelligence usually consists of a large number of facts, any one of which standing alone appears to be insignificant. However, the sum of them may be significant. To require disclosure of one, then of another, then of yet another fact would reveal to a hostile agency enough of the picture to enable it to ascertain what success the agency has had in its investigations.

- 116. The advantage of the "nature of the document" test, on the other hand, is that it is easier to apply and entails less risk of error. It asks simply, "What is the subject matter of the document?", or "To what does the document relate?" If the document relates to an exempt subject matter, then it is not to be released. This test seems particularly suited to the more sensitive areas of government policy, such as security and intelligence matters.
- 117. If a "severability" or "segregability" clause is included in freedom of information legislation, requiring a line-by-line scrutiny of classified documents and the release of all non-sensitive information, we feel that it should not apply to security and intelligence matters. It is not always easy, especially if a "damage to interest" test is being applied, to determine whether requested information falls within an exempt category. The decision becomes much more difficult when it is a matter of editing words and phrases from a sensitive file in order to release the "innocuous" parts. In the case of a file containing information obtained from a confidential source, for example, how is one to know which bits of information, individually or taken together, might provide the missing piece of data for someone who is attempting to identify the confidential source? Thus, in security and intelligence matters, a severability provision would multiply the problems involved in keeping potentially damaging information from being released.

WE RECOMMEND THAT there be a specific exemption from disclosure in freedom of information legislation of the whole of all security and intelligence documents relating to or consisting of:

- 1. security and intelligence operations
- 2. security intelligence information
- 3. information obtained from confidential sources
- 4. policy papers and intelligence analyses
- 5. manuals and directives of security and intelligence agencies
- 6. management, personnel and financial information of security and intelligence agencies
- 7. resources information
- 8. information received in confidence from foreign governments and security and intelligence agencies
- 9. structures of security and intelligence agencies
- 10. intra-governmental structural relationships
- 11. inter-governmental structural relationships

[Recommendation 31]

118. Our fourth point with regard to the drafting of a security and intelligence exemption is that the security and intelligence agency should not be required, in the case of requests for investigative reports and intelligence information, to disclose whether or not a record actually exists. We wish to avoid the situation where an individual applies for a security record concerning himself and, although he is denied his request, is in effect told that such a record exists. In this way for example, a hostile agent, could learn whether or

not a security or intelligence agency has a record of his activities. Equally important, he could find out that there is no record on him in the agency's files. The only real solution would appear to be to frame the exemption so that the refusal to inform the applicant as to the document's existence is answerable merely by reference to the information contained in the request. This would ensure that the denial relates to the request, and not to a document whose existence should remain unknown.

WE RECOMMEND THAT the freedom of information legislation provide that in responding to a request for a document or documents which fall into any of the exempt categories the government be empowered to reply that the request for such document or documents falls within such categories and the government refuses to disclose the existence or non-existence of such a document or documents.

[Recommendation 32]

119. Our fifth and final comment with regard to the drafting of security and intelligence exemptions is that, in addition to the special exemption which would apply only to security and intelligence matters, there should be a secondary "security of Canada" exemption. The phrase "security of Canada" should be carefully defined and we will be making recommendations in that regard in a later report. This general exemption would employ a "damage to the security of Canada" test, and would apply to all classes of government information. Thus if a document did not meet the subject-matter criteria of the security and intelligence exemption (or any other exemption), but could, if released, reasonably be expected to threaten the security of Canada, as carefully defined, then the information should be withheld.

WE RECOMMEND THAT any documents not included in the previously mentioned exemptions which could, if released, reasonably be expected to threaten the security of Canada, be exempted from disclosure under freedom of information legislation.

[Recommendation 33]

### Part II:

### PROTECTION OF ADMINISTRATION OF CRIMINAL JUSTICE INFORMATION FROM DISCLOSURE UNDER FREEDOM OF INFORMATION LEGISLATION

120. In the section of this report dealing with the leakage of government information we made a recommendation that it be an offence to disclose certain government information disclosure of which could adversely affect the administration of criminal justice. Clearly all such information should also be exempted from disclosure under freedom of information legislation.

WE RECOMMEND THAT any information relating to the administration of criminal justice the disclosure of which would adversely affect

- (a) the investigation of criminal offences;
- (b) the gathering of criminal intelligence on criminal organizations or individuals;
- (c) the security of prisons or reform institutions; or,
- (d) might otherwise be helpful in the commission of criminal offences be exempted from disclosure under freedom of information legislation.

[Recommendation 34]

121. In considering the mechanics which ought to apply to requests for information with respect to the security and intelligence exemptions we pointed out that the mere knowledge by an applicant of the existence or non-existence of a document or file could have serious consequences for the security of Canada. Similarly, in dealing with two of the areas relating to the administration of criminal justice exemptions, viz., (a) the investigation of criminal offences, and (b) the gathering of criminal intelligence on criminal organizations or individuals, disclosure of the existence or non-existence of a file could have a serious effect on the fight against crime. For example, knowledge by a criminal that the police were investigating him in connection with the commission of a criminal offence or were gathering intelligence on him with respect to criminal activities in general might well cause him to take actions designed to thwart the legitimate investigations by the police. We therefore think that the government, in regard to those two areas, should be allowed to neither confirm nor deny the existence of a document or file.

WE RECOMMEND THAT the freedom of information legislation provide that, in responding to a request for a document or documents which fall into the category of information relating to the administration of criminal justice the release of which would adversely affect

(a) the investigation of criminal offences, or

(b) the gathering of criminal intelligence on criminal organizations or individuals

the government be empowered to reply that the request for such document or documents falls within such categories and the government refuses to disclose the existence or non-existence of such a document or documents.

[Recommendation 35]

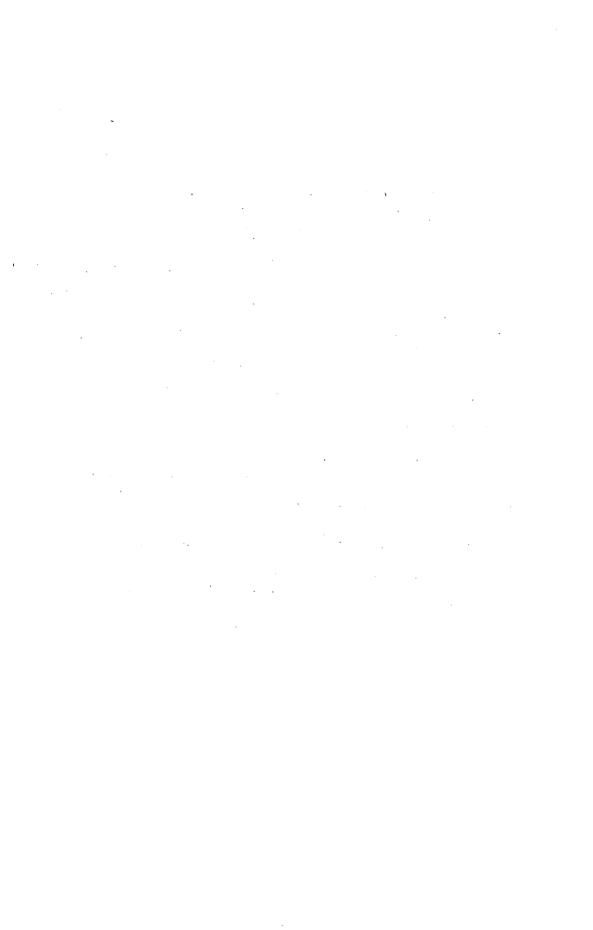
### Part III:

### A TIME LIMIT ON NON-DISCLOSURE OF SECURITY AND INTELLIGENCE INFORMATION

122. An important qualification which we would add to the suggestions outlined above concerns the effluxion of time. With respect to most, but not all, of the information in the categories for which we have recommended protection, after a certain period of time the necessity for protection would no longer exist because of drastically changed circumstances. Based on the rate of change in circumstances in the past and an educated guess as to the degree of change over time in the future, we think that the protection should be afforded to such information for a period of thirty years. We do not advocate that at the end of that thirty year period all such information be made public; rather, we feel that a "damage to interest" test should then be applied and if the release of the information could reasonably be expected to damage the security of Canada, reveal the identity of a living confidential source, or endanger life or property, then it should continue to be protected from disclosure. If, contrary to our recommendation, the "damage to interest" test were adopted in the first instance, then there would be no need for a time limitation: either release of a document, no matter how old, would damage the specified interest or it would not.

WE RECOMMEND THAT any security and intelligence document exempted from disclosure be released after a period of thirty years unless after that time its release could reasonably be expected to damage the security of Canada, reveal the identity of a confidential source, or endanger life or property.

[Recommendation 36]



### Part IV:

### **REVIEW OF GOVERNMENT DECISIONS**

- 123. We envisage review of the government's refusal to release information. The initial review would be by an administrative tribunal. That tribunal might be an Information Commissioner. In some cases there should be an appeal from the decision of the administrative tribunal to the Federal Court of Canada. There are two distinct sets of circumstances which could arise. They are:
  - (a) An applicant for information has received a response from the government that because the request relates to security and intelligence or to the administration of criminal justice the government refuses to confirm or deny the existence of the requested document. We feel that all such refusals should be referred automatically to the administrative tribunal for review as to whether the document properly fell within the category of documents for which the government was entitled to claim protection and whether the government had appropriately refused to confirm or deny the existence of the document. The decision of the administrative tribunal in such cases should be binding on the government.
  - (b) An applicant is denied access to a document on the grounds that it falls within one of the protected categories, or, if outside the categories, its disclosure would be damaging to the security of Canada. The applicant in such cases should have a right to require a review by the administrative tribunal and both the applicant and the government should have a right of appeal from a decision of the administrative tribunal to the Federal Court of Canada.

We appreciate that with respect to the "nature of the document" test the scope of the review by the administrative tribunal and any appeal to the Federal Court of Canada would be limited; nevertheless, we feel that such a review of the government's decision in these matters would be appropriate to ensure that the document truly does "relate to, or consist of" one of the specified categories. To the extent that the "damage to interest" test comes into play, the review and any subsequent appeal would determine whether the government had properly applied the relevant test. We can see no reason as a matter of principle why the government should have the final say over the release of material for the sole reason that it relates to security and intelligence matters or to the administration of criminal justice.

WE RECOMMEND THAT all decisions by the government to refuse disclosure of a document based on security and intelligence grounds or administration of criminal justice grounds be subject to review by an administrative tribunal. WE FURTHER RECOMMEND THAT such a review be automatic in those cases where the government has advised the requestor that it refuses to confirm or deny the existence of the document requested, and in all other cases the review be at the request of the person seeking the document.

WE FURTHER RECOMMEND THAT in those cases where the existence of a document is admitted to the person seeking the document, that person and the government each have a right of appeal from the administrative tribunal to the Federal Court of Canada.

[Recommendation 37]

### Part V:

# DISCLOSURE OF SECURITY AND INTELLIGENCE INFORMATION IN THE COURSE OF JUDICIAL PROCEEDINGS

- 124. Another way in which public access to security and intelligence information becomes an issue is when, in the course of judicial proceedings, one of the litigants seeks to introduce evidence consisting of information which is possessed by the federal government. What safeguards are necessary? The present section 41(2) of the Federal Court Act applies to such a situation. It provides:
  - "41. (2) When a Minister of the Crown certifies to any court by affidavit that the production or discovery of a document or its contents would be injurious to international relations, national defence or security, or to federal-provincial relations, or that it would disclose a confidence of the Queen's Privy Council for Canada, discovery and production shall be refused without any examination of the document by the court."

Such conclusive exercise of a ministerial discretion is undesirable and unnecessary. We consider that the decision whether or not security and intelligence information may be produced in open court is one which a judge is capable of making, after he has heard arguments in camera and weighed the interests at stake. We favour the procedural approach adopted in the Israeli Law of Evidence (Amendment) Law 5728-1968, which provides:

- "(a) A person is not bound to give, and the court shall not admit, evidence regarding which the Prime Minister or the Minister of Defence, by certificate under his hand, has expressed the opinion that its giving is likely to impair the security of the State, or regarding which the Prime Minister or the Minister of Foreign Affairs, by certificate under his hand, has expressed the opinion that its giving is likely to impair the foreign relations of the State, unless a judge of the Supreme Court, on the petition of a party who desires the disclosure of the evidence, finds that the necessity to disclose it for the purpose of doing justice outweighs the interest in its non-disclosure.
- (b) Where a certificate as referred to in sub-section (a) has been submitted to the court, the court may, on the application of a party who desires the disclosure of the evidence, suspend the proceedings for a period fixed by it, in order to enable the filing of a petition for disclosure of the evidence, or, if it sees fit, until the decision upon such a petition.
- (c) A person is not bound to give, and the court shall not admit, evidence regarding which a Minister, by certificate under his hand, has expressed the opinion that its giving is likely to impair an important public interest, unless the court which deals with the matter, on the

petition of a party who desires the disclosure of the evidence, finds that the necessity to disclose it for the purpose of doing justice outweighs the interest in its non-disclosure.

(d) A petition for the disclosure of evidence under subsection (a) or (c) shall be heard in camera. For the purpose of deciding upon the petition, the judge of the Supreme Court or the court, as the case may be, may demand that the evidence or its contents be brought to his knowledge, and he or it may receive explanations from the Attorney General or his representative, and from a representative of the Ministry concerned, even in the absence of the other parties.

(e) The Minister of Justice may make rules of court for the hearing of a

petition under this section."

In addition to what is provided in the Israeli Law, we feel the Judge should have the discretion to allow any party to be present at the in camera hearing, and to impose whatever conditions he deems appropriate concerning the disclosure of the information in question. While this provision with respect to the in camera proceeding is similar to that recommended by the Law Reform Commission in its proposed Evidence Code (section 43), we believe that the Israeli provision with the addition which we propose, is preferable in its details.

We think that the Federal Court of Canada would be the appropriate 125. court to decide questions of this kind that arise in judicial proceedings across Canada, no matter what court they may arise in. The Law Reform Commission recommended that such matters should, at the request of either party or upon the initiative of the trial court, be decided by a judge of the Supreme Court of Canada. We believe that the ultimate appellate court should not be asked to sit on such procedural matters at first instance. The Federal Court of Canada has established a standard of excellence and of independence, and its judges, or those designated to act in these matters, could develop a valuable expertise.

WE RECOMMEND THAT the provisions 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.

WE FURTHER RECOMMEND THAT upon such reference to the Federal Court of Canada the following procedure should apply:

- (a) The person hearing the judicial proceedings shall, upon such a reference being made, suspend the judicial proceedings until the decision on the reference is rendered.
- (b) The Federal Court of Canada shall determine whether the necessity to disclose the evidence for the purpose of doing justice outweighs the interest in its non-disclosure.

(c) The Federal Court of Canada shall hear the reference in camera. The Court may require that the evidence or its contents be brought to its knowledge. The Court may receive explanations from the Attorney General of Canada or his representative, and, if a Minister of the Crown has certified by affidavit, from the representative of that Minister, and from any party to the judicial proceedings. The Court may in its discretion allow any party to the judicial proceedings to appear at the in camera hearing and may impose whatever conditions it deems appropriate concerning disclosure of the information in question.

[Recommendation 38]



### Part VI:

### DISCLOSURE OF ADMINISTRATION OF JUSTICE INFORMATION IN THE COURSE OF JUDICIAL PROCEEDINGS

126. The disclosure in the course of judicial proceedings of the kinds of information with respect to the administration of justice dealt with by us in this report is now governed by the provisions of section 41(1) of the Federal Court Act. That section reads:

"41. (1) Subject to the provisions of any other Act and to subsection (2), when a Minister of the Crown certifies to any court by affidavit that a document belongs to a class or contains information which on grounds of a public interest specified in the affidavit should be withheld from production and discovery, the court may examine the document and order its production and discovery to the parties, subject to such restrictions or conditions as it deems appropriate, if it concludes in the circumstances of the case that the public interest in the proper administration of justice outweighs in importance the public interest specified in the affidavit."

We consider that the section provides adequate protection for all of the competing interests and we therefore have no recommendations for any changes.

1



## **CONCLUSION**

- 127. It is not our intention to express any general conclusions, as our views have been expressed already and no single thought could be said to reflect our recommendations on the wide variety of matters that this Report discusses.
- 128. This, the first Report of the Commission, will be followed in due course by other Reports concerning other matters. It is intended to postpone our expression of appreciation of the work of those who have assisted us in the preparation of this Report, until the publication of the final Report, at which time the work of all persons who will have assisted us can be acknowledged.



# SUMMARY OF RECOMMENDATIONS

1. WE RECOMMEND THAT new espionage legislation incorporate in a single enactment the offences relating to espionage now set out in section 3(1) of the Official Secrets Act and section 42(2)(b) of the Criminal Code.

[page 11]

2. WE RECOMMEND THAT espionage offences apply only to conduct which relates to the communication of information to a foreign power.

[page 13]

3. WE RECOMMEND THAT new espionage legislation define the term "foreign power" to include a foreign group that has not achieved recognition as an independent state.

[page 13]

4. WE RECOMMEND THAT new espionage legislation cover the disclosure of, or an overt act with the intention to disclose, information whether accessible to the public or not, either from government sources or private sources if disclosure is, or is capable of being, prejudicial to the security of Canada.

[page 15]

5. WE RECOMMEND THAT new espionage legislation include the following basic provision with respect to the offence of espionage:

No person shall:

- (a) obtain, collect, record or publish any information with the intent of communicating such information to a foreign power, or
- (b) communicate information to a foreign power,

if such person knows that the foreign power will or might use such information for a purpose prejudicial to the security of Canada or acts with reckless disregard of the consequences of his actions to the security of Canada.

[page 16]

6. WE RECOMMEND THAT the provisions of section 3(1) (a) of the Official Secrets Act relating to a prohibited place be repealed and not be included in new legislation.

[page 18]

7. WE RECOMMEND THAT the provisions of section 8 of the Official Secrets Act, the harbouring section, be retained but that the new legislation should make it clear that the provisions would only apply in cases in which the accused has knowledge that the person on his premises has committed or is about to commit an espionage offence.

[page 18]

8. WE RECOMMEND THAT the new legislation include the offence of possession of instruments of espionage. Under this provision it would be an offence to be found in possession without lawful excuse of instruments of espionage, which would include false documents of identity.

[page 19]

9. WE RECOMMEND THAT new legislation with respect to the disclosure of government information should make it an offence to disclose without authorization government information relating to security and intelligence.

[page 24]

10. WE RECOMMEND THAT new legislation should empower the court trying an offence of unauthorized disclosure of government information relating to security and intelligence to review the appropriateness of the security classification assigned to such government information.

[page 24]

- 11. WE RECOMMEND THAT new legislation with respect to the unauthorized disclosure of government information should make it an offence to disclose government information relating to the administration of criminal justice the disclosure of which would adversely affect:
  - (a) the investigation of criminal offences;
  - (b) the gathering of criminal intelligence on criminal organizations or individuals;
  - (c) the security of prisons or reform institutions;

or might otherwise be helpful in the commission of criminal offences.

[page 24]

12. WE RECOMMEND THAT it should be a defence to such a charge if the accused establishes that he believed, and had reasonable grounds for believing, the disclosure of such information was for the public benefit.

[page 25]

- 13. WE RECOMMEND THAT the offence of unauthorized disclosure of government information relating to security and intelligence and the administration of criminal justice provide that a person shall not be convicted
  - (a) if he had reasonable grounds to believe and did believe that he was authorized to disclose such information, or,
  - (b) if he had such authorization, which authorization may be express or implied.

[page 25]

14. WE RECOMMEND THAT the communication of government information relating to security and intelligence or the administration of criminal justice by a person who receives such information, even though such information is unsolicited, be an offence.

[page 26]

15. WE RECOMMEND THAT it be an offence to retain government documents relating to security and intelligence or to the administration of criminal justice notwithstanding that such documents have come into the possession of a person unsolicited and that there has been no request for the return of such documents.

[page 26]

16. WE RECOMMEND THAT the failure to take reasonable care of government information relating to security and intelligence or to the administration of criminal justice not be an offence unless such conduct shows wanton or reckless disregard for the lives or property of other persons.

[page 27]

17. WE RECOMMEND THAT the consent of the Attorney General of Canada be required for the prosecution of espionage offences, conspiracy to commit espionage offences, or offences relating to the unauthorized disclosure of that federal government information discussed in this report. Similarly, the conduct of such prosecutions should be the responsibility of the Attorney General of Canada.

[page 29]

- 18. WE RECOMMEND THAT with respect to section 14(2) of the Official Secrets Act which permits *in camera* proceedings that:
  - (a) the provisions of section 14(2) be retained and made applicable to all offences, either offences in new legislation or in the Criminal Code, in which the Crown may be required to adduce evidence the disclosure of which would be prejudicial to the security of Canada or to the proper administration of criminal justice.
  - (b) the phrase "prejudicial to the interest of the state" read "prejudicial to the security of Canada or to the proper administration of criminal justice."
  - (c) the last clause of the section read "but except for the foregoing, the trial proceedings, including the passing of sentence, shall take place in public."
  - (d) the legislation make provision for the holding of an in camera pre-trial conference for the purpose of dealing with procedural questions relating to the handling of evidence which might have to be received in camera.

[page 31]

19. WE RECOMMEND THAT offences dealing with espionage and the unauthorized disclosure of information relating to security and intelligence and the administration of criminal justice should be required to be tried by indictment and not by summary conviction.

[page 32]

20. WE RECOMMEND THAT the Crown have no special right to "vet" a jury in security cases over and above the rights now provided in the Criminal Code and under provincial law.

[page 32]

21. WE RECOMMEND THAT new legislation provide that jurors who participate in proceedings *in camera* be subject to the offences relating to the unauthorized disclosure of government information.

[page 33]

22. WE RECOMMEND THAT the maximum penalty for espionage be life imprisonment, except in the case of the communication to a foreign power of information accessible to the public in which case the maximum penalty should be six years.

[page 33]

23. WE RECOMMEND THAT the maximum penalty in a case of unauthorized disclosure of government information relating to security and intelligence or the administration of criminal justice, be six years.

[page 33]

24. WE RECOMMEND THAT the presumption in favour of the Crown in section 3 of the Official Secrets Act not be incorporated in the new legislation.

[page 35]

25. WE RECOMMEND THAT the offence of doing an act preparatory to the commission of an offence under the Official Secrets Act be removed but that the other offences found in section 9 be retained in the new legislation and made applicable to the offences of espionage and the unauthorized disclosure of government information relating to security and intelligence and the administration of criminal justice.

[page 36]

26. WE RECOMMEND THAT the provisions of sections 13(a) and 13(b) of the Official Secrets Act which make the Act applicable to offences committed abroad be retained in the new legislation.

[page 36]

27. WE RECOMMEND THAT the Official Secrets Act be repealed and replaced with new legislation with respect to espionage, which should be incorporated in a new statute or placed in one part of the Criminal Code with all other national security offences.

[page 37]

28. WE RECOMMEND THAT the legislative provisions with respect to the unauthorized disclosure of information relating to security and intelligence and the administration of criminal justice be clearly separated from the legislative provisions with respect to espionage.

[page 37]

29. WE RECOMMEND THAT there be a specific exemption from disclosure in freedom of information legislation for certain security and intelligence documents.

[page 47]

30. WE RECOMMEND THAT the exemption for security and intelligence documents extend to all departments and agencies of the government.

[page 47]

- 31. WE RECOMMEND THAT there be a specific exemption from disclosure in freedom of information legislation of the whole of all security and intelligence documents relating to or consisting of:
  - 1. security and intelligence operations
  - 2. security intelligence information
  - 3. information obtained from confidential sources
  - 4. policy papers and intelligence analyses
  - 5. manuals and directives of security and intelligence agencies

- 6. management, personnel and financial information of security and intelligence agencies sources information
- 8. information received in confidence from foreign governments and security and intelligence agencies
- 9. structures of security and intelligence agencies
- 10. intra-governmental structural relationships
- 11. inter-governmental structural relationships

[page 48]

32. WE RECOMMEND THAT the freedom of information legislation provide that in responding to a request for a document or documents which fall into any of the exempt categories the government be empowered to reply that the request for such document or documents falls within such categories and the government refuses to disclose the existence or non-existence of such a document or documents.

[page 49]

33. WE RECOMMEND THAT any documents not included in the previously mentioned exemptions which could, if released, reasonably be expected to threaten the security of Canada, be exempted from disclosure under freedom of information legislation.

[page 49]

- 34. WE RECOMMEND THAT any information relating to the administration of criminal justice the disclosure of which would adversely affect
  - (a) the investigation of criminal offences;
  - (b) the gathering of criminal intelligence on criminal organizations or individuals;
  - (c) the security of prisons or reform institutions; or,
  - (d) might otherwise be helpful in the commission of criminal offence's

be exempted from disclosure under freedom of information legislation.

[page 51]

- 35. WE RECOMMEND THAT the freedom of information legislation provide that, in responding to a request for a document or documents which fall into the category of information relating to the administration of criminal justice which would adversely affect
  - (a) the investigation of criminal offences, or
  - (b) the gathering of criminal intelligence on criminal organizations or individuals

the government be empowered to reply that the request for such document or documents falls within such categories and the government refuses to disclose the existence or non-existence of such a document or documents.

[page 51]

36. WE RECOMMEND THAT any security and intelligence document exempted from disclosure be released after a period of thirty years unless after that time its release could reasonably be expected to damage the security of Canada, reveal the identity of a confidential source, or endanger life or property.

[page 53]

37. WE RECOMMEND THAT all decisions by the government to refuse disclosure of a document based on security and intelligence grounds or administration of criminal justice grounds be subject to review by an administrative tribunal.

WE FURTHER RECOMMEND THAT such a review be automatic in those cases where the government has advised the requestor that it refuses to confirm or deny the existence of that document requested, and in all other cases, the review be at the request of the person seeking the document.

WE FURTHER RECOMMEND THAT in those cases where the existence of a document is admitted to the person seeking the document, that person and the government each have a right of appeal from the administrative tribunal to the Federal Court of Canada.

[page 55]

- 38. WE RECOMMEND THAT the provisions 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.

WE FURTHER RECOMMEND THAT upon such reference to the Federal Court of Canada the following procedure should apply:

- (a) The person hearing the judicial proceedings shall, upon such a reference being made, suspend the judicial proceedings until the decision on the reference is rendered.
- (b) The Federal Court of Canada shall determine whether the necessity to disclose the evidence for the purpose of doing justice outweighs the interest in its non-disclosure.
- (c) The Federal Court of Canada shall hear the reference in camera. The Court may require that the evidence or its contents be brought to its knowledge. The Court may receive explanations from the Attorney General of Canada or his representative, and, if a Minister of the Crown has certified by affidavit, from the representative of that Minister, and from any party to the judicial proceedings. The Court may in its discretion allow any party to the judicial proceedings to appear at the in camera hearing and may impose whatever conditions it deems appropriate concerning disclosure of the information in question.

[page 58]

# P.C. 1977-1911

# CERTIFIED TO BE A TRUE COPY OF A MINUTE OF A MEETING OF THE COMMITTEE OF THE PRIVY COUNCIL, APPROVED BY HIS EXCELLENCY THE GOVERNOR GENERAL ON THE 6TH OF JULY, 1977.

WHEREAS it has been established that certain persons who were members of the R.C.M.P. at the time did, on or about October 7, 1972, take part jointly with persons who were then members of la Sûreté du Québec and la Police de Montréal in the entry of premises located at 3459 St. Hubert Street, Montreal, in the search of those premises for property contained therein, and in the removal of documents from those premises, without lawful authority to do so;

WHEREAS allegations have recently been made that certain persons who were members of the R.C.M.P. at the time may have been involved on other occasions in investigative actions or other activities that were not authorized or provided for by law;

WHEREAS, after having made inquiries into these allegations at the instance of the Government, the Commissioner of the R.C.M.P. now advises that there are indications that certain persons who were members of the R.C.M.P. may indeed have been involved in investigative actions or other activities that were not authorized or provided for by law, and that as a consequence, the Commissioner believes that in the circumstances it would be in the best interests of the R.C.M.P. that a Commission of Inquiry be set up to look into the operations and policies of the Security Service on a national basis;

WHEREAS public support of the R.C.M.P. in the discharge of its responsibility to protect the security of Canada is dependent on trust in the policies and procedures governing its activities;

AND WHEREAS the maintenance of that trust requires that full inquiry be made into the extent and prevalence of investigative practices or other activities involving members of the Royal Canadian Mounted Police that are not authorized or provided for by law.

THEREFORE, the Committee of the Privy Council, on the recommendation of the Prime Minister, advise that, pursuant to the Inquiries Act, a Commission do issue under the Great Seal of Canada, appointing

Mr. Justice David C. McDonald of Edmonton, Alberta

Mr. Donald S. Rickerd of Toronto, Ontario

Mr. Guy Gilbert of Montreal, Quebec

be Commissioners under Part I of the Inquiries Act:

- (a) to conduct such investigations as in the opinion of the Commissioners are necessary to determine the extent and prevalence of investigative practices or other activities involving members of the R.C.M.P. that are not authorized or provided for by law and, in this regard, to inquire into the relevant policies and procedures that govern the activities of the R.C.M.P. in the discharge of its responsibility to protect the security of Canada;
- (b) to report the facts relating to any investigative action or other activity involving persons who were members of the R.C.M.P. that was not authorized or provided for by law as may be established before the Commission, and to advise as to any further action that the Commissioners may deem necessary and desirable in the public interest: and
- (c) to advise and make such report as the Commissioners deem necessary and desirable in the interest of Canada, regarding the policies and procedures governing the activities of the R.C.M.P. in the discharge of its responsibility to protect the security of Canada, the means to implement such policies and procedures, as well as the adequacy of the laws of Canada as they apply to such policies and procedures, having regard to the needs of the security of Canada.

#### The Committee further advise that the Commissioners:

- 1. be authorized to adopt such procedures and methods as the Commissioners may from time to time deem expedient for the proper conduct of the inquiry;
- be directed that the proceedings of the inquiry be held in camera in all matters relating to national security and in all other matters where the Commissioners deem it desirable in the public interest or in the interest of the privacy of individuals involved in specific cases which may be examined;
- 3. be directed, in making their report, to consider and take all steps necessary to preserve
  - (a) the secrecy of sources of security information within Canada; and
  - (b) the security of information provided to Canada in confidence by other nations;
- 4. be authorized to sit at such time and at such places as they may decide from time to time, to have complete access to personnel and information available in the Royal Canadian Mounted Police and to be provided with adequate working accommodation and clerical assistance;
- 5. be authorized to engage the services of such staff and technical advisers as they deem necessary or advisable and also the services of counsel to aid them and assist in their inquiry at such rates of remuneration and reimbursement as may be approved by the Treasury Board;

- 6. be directed to follow established security procedures with regard to their staff and technical advisers and the handling of classified information at all stages of the inquiry;
- 7. be authorized to exercise all the powers conferred upon them by section 11 of the Inquiries Act; and
- 8. be directed to report to the Governor in Council with all reasonable dispatch and file with the Privy Council Office their papers and records as soon as reasonably may be after the conclusion of the inquiry.

The Committee further advise that, pursuant to section 37 of the Judges Act, His Honour Mr. Justice McDonald be authorized to act as Commissioner for the purposes of the said Commission and that Mr. Justice McDonald be the Chairman of the Commission.

Certified to be a true copy
H. Chassé
Assistant Clerk of the Privy Council

# PROSECUTIONS UNDER THE OFFICIAL SECRETS ACT"

The Canadian prosecutions for Breaches of the Official Secrets Act or for conspiracy to breach the Act are:

- 1. R. v. Rose (1947) 3 D.L.R. 618 (Quebec C.A.), convicted 6 years.
- 2. R. v. Lunan (1947) 3 D.L.R. 710 (Ontario C.A.), convicted.
- 3. R. v. Smith (1947) 3 D.L.R. 798 (Ontario C.A.), convicted.
- 4. R. v. Mazerall (1946) O.R. 511 (High Court), 762 (C.A.), convicted.
- 5. R. v. Willsher (c. 1946) unreported, convicted.
- 6. R. v. Gerson (1948) 3 D.L.R. 280 (Ontario C.A.), conviction quashed on appeal.
- 7. R. v. Woikin (1946) 1 C.R. 224, convicted, 2 1/2 years.
- 8. R. v. Boyer (1948) 7 C.R. 165 (Quebec C.A.) convicted.
- 9. R. v. Carr (1949) unreported, convicted, 6 years.
- 10. R. v. Adams (c. 1946) unreported, but see (1946) 86 C.C.C. 425 (on application for change of venue), acquitted.
- 11. R. v. Nightingale (c. 1946) unreported, but see (1946) 87 C.C.C. 143 (a contempt of court conviction upheld on appeal), acquitted.
- 12. R. v. Shuger (c. 1946) unreported, acquitted.
- 13. R. v. Chapman (c. 1946) unreported, acquitted.
- 14. R. v. Poland (c. 1946) unreported, acquitted.
- 15. R. v. Halperin (c. 1946) unreported, acquitted.
- 16. R. v. Benning (1947) 3 D.L.R. 908 (Ontario C.A.), conviction quashed on appeal.
- 17. R. v. Harris (1947) 4 D.L.R. 796 (Ontario C.A.) conviction reversed on appeal.
- 18. R. v. Biernacki (1961) unreported, but see (1962) 37 C.R. 226 (motion to quash a preferred indictment), charge dismissed at preliminary inquiry.
- 19. R. v. Featherstone (1967) unreported, convicted, 2 1/2 years.
- 20. R. v. Treu (1978) convicted, 2 years; (reversed on appeal to the Quebec Court of Appeal February 20, 1979.)

#### Related cases include:

- 1. R. v. Pochon; R. v. French (1946) 87 C.C.C. 38 (Ontario High Court).
- 2. R. v. Bronny (1940) 74 C.C.C. 154 (B.C.C.A.) (under s. 16 of Def. of Can. Regs.).
- 3. R. v. Jones (1942) 77 C.C.C. 187 (N.S.C.A.) (under s. 16 of Def. of Can. Regs.).
- 4. R. v. Samson (1977) 35 C.C.C. (2d) 258 (Quebec C.A.).

<sup>\*\*</sup>includes conspiracy to breach the Act brought under the Code.

#### Excerpts from Bill No. 248 (1978-79)

# A BILL FOR AN ACT RELATING TO THE AUSTRALIAN SECURITY INTELLIGENCE ORGANIZATION

4. In this Act, unless the contrary intention appears —

"activities prejudicial to security" includes any activities concerning which Australia has responsibilities to a foreign country as referred to in paragraph (b) of the definition of "security" in this section;

"domestic subversion" means activities of the kind to which subsection 5(1) applies;

"security" means —

- (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from
  - (i) espionage;
  - (ii) sabotage;
  - (iii) subversion;
  - (iv) active measures of foreign intervention; or
  - (v) terrorism,

whether directed from or committed within, Australia or not; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the sub-paragraphs of paragraph (a);

"terrorism" includes ---

- (a) acts of violence for the purpose of achieving a political objective in Australia or in a foreign country (including acts of violence for the purpose of influencing the policy or acts of a government in Australia or in a foreign country);
- (b) training, planning, preparations or other activities for the purposes of violent subversion in a foreign country or for the purposes of the commission in a foreign country of other acts of violence of a kind referred to in paragraph (a);
- (c) acts that are offences punishable under the Crimes (Internationally Protected Persons) Act 1976; or
- (d) acts that are offences punishable under the Crimes (Hijacking of Aircraft) Act 1972 or the Crimes (Protection of Aircraft) Act 1973.
- 5. (1) For the purposes of this Act, the activities of persons, other than activities of foreign origin or activities directed against a foreign government, that are to be regarded as subversion are—
  - (a) activities that involve, will involve or lead to, or are intended or likely ultimately to involve or lead to, the use of force or violence or other unlawful acts (whether by those persons or by others) for the

- purpose of overthrowing or destroying the constitutional government of the Commonwealth or of a State or Territory;
- (b) activities directed to obstructing, hindering or interfering with the performance by the Defence Force of its functions or the carrying out of other activities by or for the Commonwealth for the purposes of security or the defence of the Commonwealth; or
- (c) activities directed to promoting violence or hostility between different groups of persons in the Australian community so as to endanger the peace, order or good government of the Commonwealth.
- (2) For the purposes of this section, "activities of foreign origin" means activities of, directed or subsidized by, or undertaken in active collaboration with, a foreign power or foreign political organization, whether carried on or to be carried on in Australia or outside Australia.
- (3) Nothing in this section affects the meaning of the expression "subversion" in relation to activities of foreign origin or activities directed against a foreign government.

# **Footnotes**

- 1. See Appendix I.
- 2. The citations for these cases will be found in Appendix II which is a list of prosecutions under the 1939 Act.
- 3. (1974) A.C. 763, 790.



## DUE DATE

27/9/25			
08 mar 00			
3/05/24	sΨ		
A 2. 200	4		
1 02 7 200	7		
13/10/20	7		
Stulling	2		
1	<del>74</del>		
5/07/2	NZ	,	
1401/4			
	201-6503		Printed in USA

HV7641/.A3/C3/no.1
McDonald, D. C. (David C.)
Security and information:
first report / Commission
ACOJ c. 1 aa PCO

