

SUBMISSIONS TO -

Special Committee of the Senate  
on  
The Canadian Security Intelligence Service

RE -

Bill C-157  
National Security

FROM -

Canadian Civil Liberties Association

DELEGATION -

A. Alan Borovoy  
(General Counsel)  
  
Professor Ken Swan  
(Vice-President)

Ottawa

September 12, 1983

## C O N T E N T S

Introduction	page....i
The Susceptibility to Intrusive Surveillance	page....1
Electronic Bugging	page....8
Surreptitious Entry	page...12
Mail Opening	page...14
Invasion of Confidential Records	page...16
Informing and Infiltrating	page...18
The Issue of Lower Surveillance Standards	page...21
The Retention and Disclosure of Surveillance Data	page...23
The Issue of a Civilianized Security Service	page...25
The Issue of Permissible Law Breaking	page...27
The Issue of Permissible Counteraction	page...31
Safeguards and Controls	page...33
Summary of Recommendations	page...36
Notes	page...40

## Introduction

The Canadian Civil Liberties Association is a national organization with more than fifty-five hundred individual members, nine affiliated chapters across the country, and some twenty associated group members which, themselves, represent several thousands of people. A wide variety of persons and occupations is represented in the ranks of our membership - lawyers, academics, homemakers, trade unionists, journalists, media performers, minority group leaders, etc.

Among the objectives which inspire the activities of our organization is the quest for legal safeguards against the unreasonable invasion by public authority of the freedom and dignity of the individual. It is not difficult to appreciate the relationship between this objective and the subject matter of Bill C-157. In crucial respects, the Bill would permit substantial encroachments upon the fundamental freedoms of the individual.

At this point, it is important that the Canadian Civil Liberties Association articulate some of the otherwise "inarticulate major premises" which relate to this issue. In the troubled and dangerous world of to-day, we do not, indeed we cannot, object to the establishment of a special agency to perform security and intelligence functions. A combination of Soviet expansionism, international terrorism, and our own unhappy experience with made-in-Canada terrorism has rendered unacceptably foolish any suggestion that this country has no need of the kind of service which is at issue here. Moreover, we agree with the need for statutory controls on the security service. These operations have been conducted for too long on the basis of administrative fiat and makeshift ground rules.

But the endorsement of the goal does not carry with it a carte blanche for the means. The lessons of history demonstrate all too well the ease with which national security has been invoked improperly to curtail personal liberty. Sometimes such invocation has served the interests of self-seeking despots; sometimes it has merely concealed the misjudgments of well meaning zealots. Whatever the motives, the results have often meant a needless loss of liberty.

It is essential, therefore, that any statute on this subject must be drawn with the utmost care and circumspection. The powers which it creates should be confined to what is demonstrably necessary for the country's genuine security needs. The safeguards which it adopts should be sufficiently workable to reduce and, if necessary, redress any abuses of those powers. In short, the viability of our democracy requires that the security operations of government be kept in check. The need for this restraint increases with the amount of secrecy which may be involved. This factor, of course, is critical in the operations of a security and intelligence agency. The very nature of the functions at issue precludes the kind of open public scrutiny which attaches to so many other government activities. Indeed, the process surrounding the enactment of such a statute might well represent the last practical opportunity for many members of the public to influence the shape of Canada's security functions. Once the statute is enacted and proclaimed, the agency could effectively disappear from public view.

By now, we suspect that our organization's general response to Bill C-157 is well known to the members of this Committee. We believe that the powers the Bill would create are excessive and the safeguards it would adopt are inadequate. Overbroad definitions of what constitutes a threat to the security of Canada would suffice to trigger a host of intrusive powers of surveillance. Little or no attempt is made to gear the investigative response to the magnitude of the threat. Virtually anything which falls within the wide definitions can justify virtually any of the surveillance techniques involved.

The ensuing submissions are an attempt to redress much of this imbalance. Consistent with this aim, we shall attempt in numbers of situations to recommend specific alternatives. Since our brief is addressed essentially to the narrow arena of national security, it takes a restricted position on many of the broad issues it confronts. With regard to a number of investigative techniques, for example, we argue that the security power should be no greater than the general law enforcement power. It should not be assumed from this that we are content with the state of the general law. In many respects, we believe that the existing criminal law grants the police too much power. But a brief dealing with security matters is not the appropriate forum for the exploration of so large an issue. The fulfilment of that objective will continue to occupy us in other contexts.

Since the Committee's guidelines for public submissions included a request for brevity, it will also be understood that this brief does not aim to be comprehensive. The emphasis here is on concept rather than detail.

## The Susceptibility to Intrusive Surveillance

Under Bill C-157, the new security and intelligence agency will have far too much intrusive snooping power - electronic bugging, surreptitious searches, mail opening, and invasion of confidential records.

In common with the Official Secrets Act and the 1975 mandate, Bill C-157 would permit such intrusive surveillance techniques to be used for "activities directed toward" certain types of security related misconduct. What is the scope of the quoted words? To what extent could they invite speculation about security threats which might happen at some indefinite point in the future? How far could such speculation justify surreptitious snooping into the private affairs of Canadian citizens even though the "activities" triggering the surveillance are completely lawful? Nowhere does the Bill require that the targetable "activities" be unlawful.

Consider, for example, the power the Bill would create for intrusive snooping into "activities within...Canada directed toward or in support of...acts of violence... for the purpose of achieving a political objective within Canada or a foreign state". How far would this section mandate the use of intrusive surveillance against a group of Canadian citizens who were merely fund raising to help the Afghan rebels chase the Soviet army out of their country? Or speech making in support of the British position in the war over the Falkland Islands or the Israeli invasion of Lebanon?

A later sub section would permit intrusive surveillance into "activities...intended ultimately to lead to the destruction or overthrow of the constitutionally established system of government in Canada". How far would this provision permit the targeting of a group which harboured fantasies about world revolution but whose current and foreseeable activities involved nothing more than pamphleteering and impotent preaching? Significantly, the McDonald Commission had recommended that such groups be monitored only by non intrusive techniques. And, to what extent might this section permit intrusive surveillance against democratic separatists and world federalists? Since they are working for the replacement of our constitutional system by something radically different, could it be said that they are intending ultimately to "overthrow" the established arrangements? This interpretation is bolstered by the fact that the same sub section refers earlier to "activities directed toward undermining by

covert unlawful acts" the established constitutional system. Since unlawful methods are specifically required for "undermining" but not for "overthrowing", the latter might well contemplate lawful methods as well.

Another factor which tends to create overbroad powers is the subjectivity and vagueness of the expressions. Intrusive surveillance will be permitted into "foreign influenced activities...that are detrimental to the interests of Canada or any state allied or associated with Canada...". "Influence" covers a lot of territory. If the Canadian Civil Liberties Association draws inspiration from the American Civil Liberties Union, does this mean that our organization is "foreign influenced"? What are the limits of "detrimental"? Suppose a Canadian citizen were employed by a foreign corporation which was involved in commercial negotiations with the Government of Canada? Since it might be in the interests of Canada to sell high and buy low, would any opposite interest be considered "detrimental"? On this basis, could a Canadian citizen in such a position have his conversations bugged, premises searched, mail opened, and records invaded? The subsequent requirement in the section that the activities be "clandestine or deceptive" may not adequately diminish the danger. There is an element of the clandestine in virtually all commercial transactions.

Moreover, what is a state "associated with" Canada? Since the section also uses the term "allied with", "associated with" must mean something different. Arguably, Canada might be "allied with" the United States in NATO and "associated with" the Soviet Union in the United Nations. How far, then, might this section permit intrusive surveillance of Canadian citizens who were pursuing interests detrimental to those of the Soviet Union?

On the basis of another section, intrusive surveillance will be permitted in order to acquire information about the "capabilities, intentions, or activities" of foreign states and persons. But, while the information at issue must be about foreigners, it could be obtained from citizens. Presumably, therefore, innocent Canadian citizens might be subject to all this snooping simply because they may have some knowledge or expertise about foreign countries. Imagine the consequent vulnerability of businessmen involved in international commerce, trade unionists with foreign contacts, and even ordinary well-travelled tourists.

And how far could all these techniques of intrusive surveillance be used to assist the security service in "remaining informed about the political, economic, and social environment within Canada..."? (section 14[2]). To what extent might it be argued that the exercise of "remaining informed" is enough of a "duty" or at least a "function" (section 22) of the Service in order to justify its acquisition of a warrant for electronic bugging, mail opening, surreptitious entry, or the invasion of confidential records? At best, the terminology of the Bill in this area is dangerously unclear.

Despite the government's attempts to assure us, this Bill must be seen, therefore, as a threat to law-abiding people and legitimate dissent. In the opinion of the Canadian Civil Liberties Association, this threat will continue so long as intrusive surveillance is permitted on the basis of such shadowy, ethereal, and overbroad concepts as "activities directed toward", "ultimate" intentions, "detrimental" interests, and "associated" states.

Nor are these dangers sufficiently diminished by the requirement in section 14[3] which specifies that there is no authority to investigate any person or group "solely on the basis of the participation by that person or group in lawful advocacy, protest or dissent". While the word "solely" may be necessary, it nevertheless could vitiate the restrictive purposes of this limiting clause. Inevitably, the argument will be made that it is not "solely" the lawful advocacy which triggers the surveillance in question; it is also the suspicion of what the advocacy is "directed toward".

At base, it is difficult to square the powers in Bill C-157 with the democratic philosophy. Generally, democratic societies have believed that their citizens should be immune from intrusive encroachments unless law-breaking is likely involved. Under the Criminal Code, for example, there cannot be wiretaps, entries, searches, seizures, or arrests without reasonable grounds to suspect certain criminal offences. Why, then, so wide an exemption for presumed, remote, or even imagined threats to the national security? Why should intrusive surveillance be permissible in the security area for "activities directed toward" certain apprehended conduct even though there may not be a stitch of evidence that the law is being violated?

No doubt we will be told that the special role of security intelligence is to prevent the apprehended harms before the country suffers them. As attractive as this approach might initially appear, the dangers must be appreciated. Preventive intelligence gathering could well encourage the most groundless of anticipatory speculation. When surveillance is addressed to "activities directed toward", there is a real risk that it will embrace completely lawful conduct. The detection of misconduct long in advance of its actual commission may require not only discernment but also clairvoyance. Moreover, when the goal is prevention the idea is to amass enough intelligence to make reliable predictions. Thus, there could be a tendency to intrude very pervasively on the targets of the investigations - to learn as much as possible about their habits, beliefs, associations, and predilections. It is not hard to appreciate the potentially chilling impact of such an approach on the rights of privacy and dissent.

Moreover, there is good reason to question how much additional security is obtained through such preventive intelligence gathering. In this regard, the experience of the American FBI is instructive. Comprehensive audits performed by the independent General Accounting Office of the U.S. Congress found that, despite a relatively unencumbered mandate, "generally the FBI did not report advance knowledge of planned violence".<sup>1</sup> In 1974, for example, the GAO estimated that the FBI obtained advance knowledge of its targets' activities in only about 2% of its investigations. And most of this knowledge related to completely lawful activities such as speeches, meetings, and peaceful demonstrations.<sup>2</sup> According to a member of the U.S. Senate Intelligence Committee, "The FBI only provided...a handful of substantiated cases - out of the thousands of Americans investigated - in which preventive intelligence produced warning of terrorist activity".<sup>3</sup> And a former White House official, with special responsibilities in this area, declared that "advance intelligence about dissident groups (was not)... of much help" in coping with the urban violence of the 1960's.<sup>4</sup>

Accordingly, American law-makers have adopted a number of measures to restrict the scope of the FBI's preventive intelligence gathering. Where domestic threats are concerned, the FBI has been operating under unprecedentedly strict guidelines since 1976. While these guidelines have been somewhat broadened under the Reagan administration, they appear nevertheless to have retained certain key features, for example, -

"the critical requirement of a link to federal criminal law as a predicate to investigation".<sup>5</sup> Since 1972, electronic surveillance against domestic threats has been conducted entirely under the authority of a general statute which requires probable cause to believe that certain crimes are involved.<sup>6</sup> While a special statute was enacted in 1978 to permit electronic bugging against foreign threats, it is remarkable for its relative lack of preventive scope. Where certain foreign influences are concerned, for example, citizens and resident aliens cannot be subjected to electronic bugging within the United States unless it is likely that the activities at issue "involve or are about to involve" a federal crime.<sup>7</sup>

While not all of the intrusive techniques have been equally circumscribed, the United States has experienced a discernible trend in the above direction. In an increasing number of situations, Americans cannot be subjected to intrusive surveillance unless illegality is indicated. In view of such developments in the leading country of the Western alliance, it ill behoves Canada to adopt the kind of posture reflected in Bill C-157. In any event, the case simply has not been made for the breadth of surveillance powers which are at issue here.

For all of these reasons, we believe that the security service should not be permitted to employ intrusive surveillance against citizens and permanent residents unless, at the very least, a serious security-related breach of the law is involved. We have added a "serious" requirement in order to avoid the potential trivialization of the security activity. Suppose, for example, there were a plan to throw rotten tomatoes at the Prime Minister? Or a conspiracy to pour discolouring fluids on the parliamentary carpet? Not very pleasant prospects, to be sure. While they may well be worthy, at some stage, of a law enforcement response, they hardly justify the intrusive surveillance of a security service. For such purposes, the misconduct at issue should involve serious security-related law breaking such as sabotage, espionage, or serious violence impairing the operations of government. While some forms of intrusive surveillance should require even additional conditions, none should be allowed on the basis of anything less.<sup>8</sup>

And, unlike what is permitted in Bill C-157, there should be an ongoing requirement in every situation to evaluate the security benefits against the civil liberties costs. How necessary is the intelligence which is being sought? Even for such purposes, how necessary is the surveillance technique at issue? Might something less intrusive attain the legitimate security objective? The governing statute should make such a balancing exercise the invariable prerequisite of permitting intrusive surveillance.

Moreover, there are real questions about the uses and purposes which are designed to be served by the intrusive surveillance which the law will permit. Under Bill C-157, the investigations are essentially, to use the words of an American author, "free-floating, information-gathering projects". In short, the Bill contemplates intelligence rather than law enforcement investigations. The virtue of the latter approach is that the surveillance would be designed essentially to collect evidence for the purpose of prosecution. In that way, the intrusions would become relatively limited exercises. They would focus on gathering evidence of crime. An intelligence investigation, on the other hand, intrudes pervasively. Since the goal is to assess, understand, and predict, the investigation has to accumulate a lot more information. As indicated, there will be attempts to discover almost everything there is to know about the targets, including their most intimate predispositions. This is why intelligence investigations are such a danger to both political liberty and personal privacy.

Nevertheless, where threats emanate from foreign powers, there may well have to be some special latitude for a certain amount of intelligence-centred surveillance. It will often be sensible, for example, to employ tactics other than prosecution against foreign agents who break our espionage laws. Prosecution could undermine the viability of our counter-intelligence operations. It could uncover what needs to be under cover. And it would do so without commensurate benefit. The jailing of a few Soviet spies, for example, would hardly dent the Soviet capacity for espionage.

Such considerations do not as readily apply to essentially domestic threats. They are much more vulnerable than their foreign counterparts to the therapy of law enforcement. The prosecution and incarceration of a few FLQ terrorists, for example, could and did

inflict mortal wounds on that organization's activities. Of course, like everything else in the real world, it is not a stark either-or choice. We realize that there is sometimes an argument for an intelligence component even in more conventional criminal matters. The critical point, however, is that the goal of such intelligence is, sooner or later, to prosecute. This constitutes one of the essential distinctions between the domestic and much of the foreign arena.

For these reasons, it might well be advisable to treat foreign and domestic threats in separate statutes and in separate agencies. Indeed, there is little reason why domestic security matters could not be handled primarily as a component of criminal law enforcement.

Regrettably, Bill C-157 fails to make the requisite distinctions. Foreign and domestic security threats are treated almost identically. Both could give rise to the most dangerous kind of open-ended intelligence investigations. In our view, this approach endangers our liberty without proportionately enhancing our security. In short, the worst of both worlds.

## Electronic Bugging

Electronic surveillance is one of the most intrusive of the investigative techniques. Unlike the physical search of premises, the electronic bug cannot discriminate. It overhears everyone within earshot - the guilty, the suspected, and the innocent alike. By now, for example, some 1500 people have been convicted of criminal offences arising out of American police bugging in 1969 and 1970.<sup>9</sup> During the course of this surveillance, however, the American authorities overheard more than 40,000 people in more than a half a million conversations.<sup>10</sup> Undoubtedly, the overwhelming majority of these people was innocent of wrongdoing. And, apart from gambling, the overwhelming majority of intercepted conversations was non incriminating - at least 75% according to the law enforcement authorities themselves.<sup>11</sup>

In the area of security and intelligence, the dragnet character of the technique is even greater. While federal law enforcement bugs in the United States endured an average of 13.5 days and overheard an average of 56 people and 900 conversations, the average national security bug in that country lasted from 78.3 to 290.7 days and overheard somewhere between 5500 and 15,000 people.<sup>12</sup> Unfortunately, the Canadian statistics do not include the number of people and conversations intercepted. But they do reveal the length of the bugging operations. Here too a similar pattern emerges. In 1978, the average duration of a law enforcement bug was 73.5 days.<sup>13</sup> In the case of federal security bugs, it lasted as long as 244.71 days.<sup>14</sup>

In view of this enormous capacity to intrude, it is necessary to evaluate costs and benefits. Are the security benefits derived worth the privacy costs incurred? In security matters, the impact of bugging is especially difficult to measure. Unlike normal law enforcement, the prosecution and incarceration of offenders is not often the object of the exercise. Thus, there are few tangible bench marks by which to judge these eavesdropping techniques. What we do have are the opinions of several experts who have worked in the field. Significantly, a number of them have actually expressed considerable doubt about the necessity of security bugging.

Morton Halperin, a former member of the U.S. National Security Council, made the following statement.

"In my judgment, such surveillance has extremely limited value and can in no sense be called vital to the security of the United States. ...the American government has many other sources of information of significantly greater value".<sup>15</sup>

Former U.S. Attorney General Ramsay Clarke contended that, if all security bugs were turned off, the impact on security would be "absolutely zero".<sup>16</sup>

In the event that the involvement of these two commentators with the American Civil Liberties Union might generate some skepticism about their judgments, we should note the similar assessments which have emanated from people who are miles away from them on the ideological spectrum. Consider, for example, former FBI Director, the late J. Edgar Hoover.

"I don't see what all the excitement is about. I would have no hesitancy in discontinuing all techniques - technical coverage (i.e. wiretapping), microphones, trash covers, mail covers, etc. While it might handicap us, I doubt they are as valuable as some people believe and none warrant the FBI being used to justify them".<sup>17</sup>

Mr. Hoover's associate who was in charge of these matters, the late William Sullivan, recommended a few years ago that all security bugs and taps be turned off for a period of 3 years in order properly to assess their importance.<sup>18</sup> It is fair to infer that a knowledgeable official would not be likely to make such a proposal if he thought that the results would create a serious danger to American security.

In this connection, there is on the public record a most remarkable statement made by the man whose activities in these matters drove him to resign in disgrace from the most powerful office in the world - former U.S. President Richard Nixon.

"They (the taps) never helped us. Just gobs and gobs of material: gossip and bullshitting... The tapping was a very unproductive thing. I've always known that. At least, it's never been useful in any operation I've ever conducted".<sup>19</sup>

In view of the misgivings expressed by these experts, it is especially disquieting to examine the breadth of the proposed security bugging power in Bill C-157.

As far as serious political violence is concerned, why is there a need for a greater bugging power than what is already contained in the Criminal Code? At the moment, the Code permits electronic surveillance for the investigation of more than 40 criminal offences including high treason, intimidating Parliament, sabotage, highjacking, murder, arson, possession of explosives, kidnapping, extortion, and even conspiracies to commit these offences both in Canada and elsewhere.<sup>20</sup> What conceivable act of terrorism or serious political violence has been omitted from the list? On the contrary, it might be argued that the bugging power in the Criminal Code exceeds the bounds of demonstrated necessity. But where is the need for anything more?

Where the detection of espionage is concerned, the problem is pretty much the same. The formulation "activities directed toward" may be capable of including lawful conduct which occurs years before the apprehended illegality. Why is it necessary to permit such pervasive intrusions as electronic bugging on the basis of what may be remote speculation? Why would it not suffice if the bugging powers in this area were confined to illegalities concerning espionage? Why shouldn't the power to bug require, at the very least, that there be a counselling or conspiracy to commit these acts? Again, while it might be argued that such a power could include too much, there is hardly a case for anything more.

As far as foreign influenced activities are concerned, we do acknowledge that there is a case for a level of surveillance in this area. But, as we have indicated, not everything so described is likely to raise a security problem. If, of course, the foreign power resorted to certain illegalities (violence, extortion, bribery) in order to exert its influence, the transactions would already be susceptible to electronic bugging under the Criminal Code.<sup>21</sup> This would not be the case, however, if the influence were merely "clandestine". The problem is that some clandestine activities carried on by foreign powers here may truly raise issues of security while, as indicated, others do not. Some democratic countries address this problem by requiring the agents of foreign powers to undergo a procedure of registration so that they might be readily identified as such.<sup>22</sup> In that way, their activity would be less clandestine. These registration laws have been criticized by some as excessive and by others as unworkable. For the moment, we make no recommendations on this

point. Suffice it for us to insist that the prerequisite for intrusive surveillance in this area is serious law breaking. In our view, if conduct is not considered sufficiently dangerous to warrant a legal prohibition, there is a real question whether it should suffice to trigger intrusive surveillance.

Our recommendations are reinforced by the experience in the United States. As indicated, American bugging against domestic security threats is handled entirely under a general criminal statute.<sup>23</sup> And, even where foreign security threats are concerned, similar standards are required for the bugging of American citizens and resident aliens within the United States.<sup>24</sup> In view of the fact that the U.S. is the most targeted country in the democratic world, how can Canada justify so much additional authority for electronic surveillance?

Recommendation No. 1

- As regards the security bugging of Canadian citizens and permanent residents, the law should require, at the very least, reasonable grounds to suspect a serious security-related breach of the law such as sabotage, espionage, or serious violence impairing the operations of government.

Recommendation No. 2

- At least where essentially domestic security threats are concerned, bugging should be conducted entirely under the Criminal Code, subject to all of its existing safeguards.

### Surreptitious Entry

The surreptitious entry is a particularly insidious form of intrusion. It is designed essentially to permit the conduct of an intelligence probe. The security officers rummage around the premises in search of information. Unlike the law enforcement bugging operation and the search and seizure exercise under the Criminal Code, the target is very unlikely to learn what has happened. The goal of the operation is rarely the prosecution of offenders; it is usually the acquisition of intelligence.

For all the reasons we have indicated, we believe it would be repugnant to permit such insidious intrusions on any citizen or permanent resident unless, at the very least, there existed the circumstances which we had recommended for electronic bugging - reasonable grounds to suspect a serious security-related breach of the law. While nothing less, in our view, could justify a surreptitious entry, we believe it should require even more.

Although it is always difficult to compare the intrusiveness of various techniques, there are some respects in which a surreptitious entry for the purpose of a search is more dangerous than one which is committed to install a bug. In the latter case, the intruders can minimize the length of time they spend on the property; in the former case, they may have to linger until they find what they are seeking. The longer they linger, the greater the risk of a confrontation with the owner or occupant.

In our view, the only arguable case that might be made for so insidious and dangerous a power is in circumstances where there are reasonable grounds to suspect that the serious security-related breach of the law is being directed by a foreign power. As indicated, there are many situations where it would be unwise to prosecute those who are involved in wrongdoing of an international character. But there is no reason for comparable reticence where the security threats are essentially of a domestic character. Domestic organizations are more susceptible than foreign ones to immobilization through normal law enforcement processes. It more often makes sense, therefore, to prosecute and even to attempt to incarcerate such domestic law-breakers. Unlike the case with many foreign threats, entries against domestic wrongdoers should

more often be designed to gather evidence for prosecution, either by way of electronic bugging or search and seizure. In both cases, however, the domestic target should generally be told what has happened.

Again, our views are sustained by the American experience. Apart from the planting of bugs, U.S. law does not permit surreptitious entry against an essentially domestic threat.<sup>25</sup> What is even more significant is the absence of any concerted attempt to enact such a power in that country.

Moreover, even in the case of a foreign-directed operation, there is no reason to countenance, as Bill C-157 apparently does, the permanent removal of any things or materials from any premises in question. It is one thing to permit the security agents to examine property that does not belong to them; it is another thing entirely to allow them to confiscate such material. Despite all of the study which the McDonald Commission performed in this difficult area, it did not include such a proposal in its recommendations.

### Recommendation No. 3

- Apart possibly from serious security-related breaches of the law directed by a foreign power, citizens and permanent residents should be immune from surreptitious entry unassociated with electronic bugging. And, even in the case of such foreign directed operations, the security service should be required, presumptively at least, to return anything that was removed.

### Mail Opening

At the moment, mail opening in the course of post is prohibited almost entirely under Canadian law. Thus the question which must be faced is whether any mail opening power should now be permitted.

In this regard, it is significant to note the finding of the McDonald Commission with respect to its probe of past mail opening activities. The Commission concluded that the intelligence produced by these operations was of "only marginal value".<sup>26</sup> Remember too that the RCMP admitted to hundreds of illegal mail openings for at least 30 years. Yet, in all of the situations which were identified for these purposes, the Commission could find nothing more than marginal benefits. Hardly the stuff on which to base a new power of surreptitious surveillance.

In making this argument, we quite appreciate that the law already permits forms of surveillance which may be more intrusive than mail opening. In our view, however, this cannot constitute a basis for yet another encroachment on civilian privacy. Even though this Bill may represent Canada's first comprehensive legislation in this area, our society does not have the luxury of starting from scratch. We are in the middle of history and not at the beginning. Since the operative standard of democratic government is no additional encroachment without justification, the onus remains on the proponents of mail opening to demonstrate its necessity. If anything, the existence of more intrusive techniques might occasion some valid arguments against them. But, by themselves, they cannot justify the creation of a new power.

Nor do we overlook the argument made by Prime Minister Trudeau a number of years ago. Why, he asked, is it permissible to obtain a search warrant to seize a letter immediately after its delivery to the intended recipient but not moments before while it is in the course of post? The answer is that the investigation of delivered mail is more likely to be known to the target. It will require a personal visit to his premises. His likely knowledge of the investigation will serve

to reduce the incidence of abuse. Undelivered mail, however, is much more susceptible to surreptitious interception. Thus such mail openings would be subject to the kind of abuse that is not as available with the Criminal Code searches of premises.

On this basis, there could only be one situation where there might be an argument for mail opening in the course of post - where there are reasonable grounds to suspect a serious security-related breach of the law directed by a foreign power. But whatever the arguments about foreign threats, no case has been made for a mail opening power against essentially domestic threats.

And, to whatever extent such a power were created, it should be handled more like a search warrant than a wiretap authorization. Unlike the open-ended scheme which has been proposed, warrants should not issue for long periods of time in respect of broad categories of letters not yet in existence. Rather, they should be restricted, as far as possible, to particular and identifiable letters.

#### Recommendation No. 4

-Apart possibly from those situations where there are reasonable grounds to suspect a serious security-related breach of law directed by a foreign power, the law should continue to deny the security service a mail opening power against citizens and permanent residents. To whatever extent mail opening became permissible, it should be restricted as far as possible to particular and identifiable letters.

### Invasion of Confidential Records

In order to plan intelligently and provide a complex level of services, the government collects mountains of information about us - assets, debts, income, employment, aptitudes, health, sickness, family background, etc. So vital are these data regarded for government operations that in numbers of situations, the law requires that we furnish the facts which the government seeks. In many such situations, the balance between personal privacy and government "need to know" is a legal obligation on the data collectors to keep confidential the contents of individual files. The uses of the information are confined to the purposes for which it was collected.

Bill C-157 would give the security and intelligence agency access to all these data in the circumstances indicated. It is appropriate to remember that what is at issue here is special; it is in addition to the contentious powers of access which are already contained in the new Privacy Act.<sup>27</sup> Again, we believe that such access should not be permitted against citizens and permanent residents unless, at a minimum, there are reasonable grounds to suspect a serious security-related breach of the law. Indeed, there is some personal information in the hands of the government which is so delicate that, even in the circumstances of such law-breaking, it should be withheld from the security service.

The McDonald Commission recommended such immunity for census information. Bill C-157 disagrees. We believe that the Commission made a particularly strong claim for this exemption.

"While such information (census) may not be more personal than that found in some other federal data banks, the tradition in this country has been very strongly in favour of complete confidentiality of census returns. The unqualified guarantee of confidentiality helps to overcome the reluctance of Canadians to respond to inquiries about personal matters...".<sup>28</sup>

We believe there is a strong argument for applying this reasoning also to the Income Tax Act. In order to levy a proper tax upon us, the revenue authorities must have the opportunity to probe deeply into our respective circumstances. In order to keep these intrusions to a tolerable minimum, the Act requires us to complete an annual return in which we take the responsibility for disclosing what is relevant. By

and large, this works well to limit the involvement of the revenue agents in our daily lives. But a very key reason for this success is the taxpayers' confidence that the data they reveal are not generally available for anything but tax purposes. Indeed, such a restriction has existed in the law since the inception of the income tax.

It is not difficult, therefore, to understand the public indignation which was provoked by the revelations of RCMP access to tax data for non tax purposes. It was considered nothing short of a breach of faith with the Canadian taxpayer. According to the McDonald criteria, there is no reason why tax data should be substantially more accessible than census data. Tax information also enjoys a strong tradition in favour of complete confidentiality and such has been necessary to overcome taxpayer reluctance to disclose.

We are unaware that an adequate case has been made for a statutory power of investigative access to tax records for non tax purposes. Despite the revelations of past RCMP access, there is no indication that the consequent benefits to national security were great enough to outweigh the obvious civil liberties costs. Any breakdown in the tax system of self-assessment is likely to precipitate a larger measure of government intrusion in our private lives. As a practical matter, the revenue authorities will not be divested of their appropriate income. If a significant number of taxpayers begins seriously to falsify their returns, more and more people will be susceptible to government investigation. That is why it is so crucially important for taxpayers to believe that their returns will be treated in confidence.

#### Recommendation No. 5

- The security and intelligence agency should have no investigative access to census and income tax information relating to citizens and permanent residents. The agency's special access to all other such personal information in government data banks should require, at the very least, reasonable grounds to suspect a serious security-related breach of the law.

### Informing and Infiltrating

Although they represent perhaps the most prevalent of the surveillance techniques, secret informants are especially threatening to personal privacy and political liberty. Unlike the physical search and the electronic bug, the informant not only spies but he also participates. If he is sufficiently charismatic, he can effectively distort the political activities of the groups he infiltrates. Indeed, he might even provoke some of the very illegalities which he has been assigned to detect.

Apart from professional police undercover agents, informants are often unstable and disreputable people. In this connection, it is interesting to note that the attempted assassin of former U.S. President Gerald Ford was an FBI informant.<sup>29</sup> The untrustworthy character of many informants has led the intelligence agencies to assign numbers of them to the same place so that they don't know of each other. In the result, much of their time and work has involved spying on each other. At one time, for example, the FBI infiltration of the American Communist Party was so extensive that there was one informant for every 5.7 genuine members.<sup>30</sup>

In those cases where money is the chief incentive, the informants may be tempted to distort and exaggerate in order to maintain their value. If nothing much is happening, the intelligence agency is not likely to go on paying. Such considerations would contribute also to the informant becoming an agent provocateur.

Despite all these dangers, Bill C-157 is remarkably devoid of attempts to regulate the activities of informants. No doubt, the defenders of the status quo will be quick to adopt the reasoning of the U.S. Supreme Court: "The risk of being.... betrayed by an informer...is the kind of risk we necessarily assume whenever we speak".<sup>31</sup> There is, of course, some truth in this. Unlike bugs and physical searches, there is some control over whom to trust. The risk of betrayal is an unavoidable component of human intercourse.

At most, however, such arguments might militate against the amount of regulation over informants as compared to other forms of surveillance. But they cannot justify the

virtual absence of regulation. In consequence, we believe that the use of informants represents a sufficient danger to our fundamental freedoms to necessitate the adoption of some regulatory mechanisms.

It is anomalous for Bill C-157 to specify that judicial warrants are needed for some forms of intrusive surveillance while it contains virtually nothing on approving the use of informants. A technique which is at once so intrusive, threatening, and in need of such political sophistication should be accompanied by statutory requirements as to whose approval will be needed under what circumstances. Even if the law does not require the permission of a judge, it should require approval from identifiable officials at the highest level. There is simply too much at stake to leave to the vagaries of bureaucratic discretion.

The governing statute should also attempt to regulate the behaviour of informants and infiltrators. How far, if at all, and under what circumstances may they interfere in the activities and policies of the targeted groups? Even interference which is not otherwise unlawful could be very damaging to the integrity of the democratic processes. The activities and policies of certain organizations would no longer represent the free and real will of their members. Could a distinction be made, for such purposes, between interfering with the lawful and unlawful activities of the targeted groups? If so, what steps might an informant take to discourage the group's unlawful conduct and what safeguards might be adopted to ensure that such interference would not affect the group's legitimate activity?

Moreover, what steps might be taken to reduce the risk that the informant might distort, exaggerate, and perhaps even fabricate in order to enhance his value? What might be done to discourage the informant from becoming an agent provocateur? How far, if at all, should such conduct render an informant subject to criminal prosecution, civil lawsuit, and/or employment discipline? How far, if at all, should there be a defence for the wrongdoer whose misconduct is provoked or encouraged by an informant? What safeguards might be adopted to ensure that such informant misconduct is brought to light?

At some point, an informant or infiltrator may acquire access to a privileged communication. What controls should be enacted to reduce the likelihood of an informant intercepting and then disseminating material which arises in such a contentious context?

No statute which purports to establish a security and intelligence agency can afford to neglect these vital issues. The deployment of human spies represents too great a danger to the viability of the democratic processes.

Recommendation No. 6

- The governing statute should contain provisions specifying the circumstances under which informants may be deployed and the officials who must approve such deployment.

Recommendation No. 7

- The statute should also contain guidelines regulating informant behaviour during such undercover operations.

### The Issue of Lower Surveillance Standards

There are situations where the standards for surveillance need not be as high as those indicated above. The legal status of the proposed target is a relevant consideration. This country owes its greatest protections to its citizens and permanent resident aliens. It need not incur the same obligations to those who are visiting temporarily as it does to those who are staying indefinitely. There may also be practical reasons for a difference in investigative thresholds. The brevity of a visitor's stay in this country might make it much more difficult to accumulate the requisite evidence of unlawful conduct. Moreover, experience indicates that, compared to citizens and residents, a significantly higher proportion of visitors is involved in foreign intelligence activity.<sup>32</sup>

On this basis, we believe that it would be permissible to allow a somewhat broader and more preventive approach in the case of foreign visitors. In this regard, it is important to resist the tantalizing arguments of those who are urging a false egalitarianism.<sup>33</sup> Some have suggested, for example, that it is unfair to make such distinctions between residents and visitors. Their solution is to propose needlessly low standards for everyone.

Lower standards are also permissible for less intrusive techniques of surveillance. Where such methods as watching, trailing, interviewing, and source checking are involved, they need not attract the kind of exacting standards that have been recommended for the more intrusive techniques. Neither, however, should their use be as open-ended as the law now permits.

When security investigations are conducted through even such less intrusive techniques, they ought to be governed by discernible standards. Again, there might be lower standards for foreign visitors than for citizens and permanent residents. A distinction might also be drawn between preliminary and deeper investigations - the latter requiring higher standards. Moreover, the statute should specify what level of authority is needed for the various levels of investigation. Since any state surveillance involves some level of encroachment on the vital values of privacy and liberty, the decision to engage in it should not be left so completely to the exercise of bureaucratic, and possibly arbitrary, discretion.

Recommendation No. 8

- While the targeting of foreign visitors and the use of less intrusive techniques might be permitted on the basis of lower standards, the governing statute should nevertheless spell out both the applicable standards and the level of official who should be empowered to authorize the requisite techniques in the circumstances at issue.

### The Retention and Disclosure of Surveillance Data

It is difficult for the intelligence gathering exercise to discriminate between what material is important and what is not. Once an authorized investigation begins, there will be a tendency for the security agency to accumulate all of the information it can. Moreover, since the investigators cannot always assess the relevance of every piece of data, they will be tempted to retain everything they acquire. Very likely, therefore, vast amounts of irrelevant personal data will find their way into the agency's files. Yet, as the American Civil Liberties Union has observed, such information may well be "the single most effective tool for political manipulation at the disposal of the government".

It is, therefore, potentially very dangerous for any such agency of government to retain identifiable information which has been gathered from the private lives of citizens and permanent residents. Beyond the question of political manipulation, there is the question of elementary fairness. In our view, human dignity is diminished to the extent that personal data pass out of an individual's control.

For these reasons, the Canadian Civil Liberties Association regrets the relative absence of effort in Bill C-157 to restrict the retention of information which is acquired. And, while there are restrictions on what might lawfully be disclosed, there is an unavoidable risk that what comes in could well get out. It stands to reason, of course, that, if less were retained, the risk would be reduced. For all of the above reasons, we would urge that Bill C-157 be amended to include criteria for the retention of surveillance material. Such criteria should articulate a test of relevance for whatever intelligence or law enforcement functions might be appropriate. Moreover, there should be time limits on such retention (less for domestic than for foreign purposes) and an explicit requirement for the destruction of the material, and where appropriate, entire files that are not necessary or relevant for such authorized purposes.

While the Bill makes some effort to restrict the subsequent disclosure of surveillance data, it nevertheless contains a gigantic loophole. The director of the agency may disclose such information to persons in the government service if, in his opinion,

the public interest in such disclosure clearly outweighs any consequent invasion of privacy. In view of the mountains of information involved, this provision could constitute a powerful temptation to abuse. At worst, the section might become a cover for the transmission of politically intimidating gossip. Such apprehensions are compounded by the ease with which the disclosures could be made. To what extent, for example, could many of the communications be oral? And, even if there were some written record which would be subject to the scrutiny of the outside review committee, it is not inconceivable that a plausible rationale might be concocted as an explanation. This is easier to do when the lawful discretion is as wide as it is here.

In our view, therefore, this open-ended discretion should be replaced by articulated guidelines which set out the conditions under which such disclosures could be made. Again, the dissemination of material relating to domestic matters should be more tightly circumscribed than those which deal with foreign issues. Since computers render everything instantly retrievable, it would be helpful also for the resulting statute to contain at least the minimum criteria for how the material would be stored, who might have access to it, and how such access should be facilitated. While many of these details might have to be left to subsequent regulations and administrative guidelines, the statute should contain at least the necessary minimum.

#### Recommendation No. 9

- There should be more specific criteria governing the retention, disclosure, and destruction of surveillance material. Such criteria should also address how the material is to be stored, who should have access to it, and how such access should be facilitated.

### The Issue of a Civilianized Security Service

The Canadian Civil Liberties Association is concerned also about the wisdom of having Canada's security functions performed by an all-civilian agency. The further that security surveillance is removed from the discipline of law enforcement, the greater the risk of blurring the line between improper subversion and legitimate dissent. The virtue of the law enforcement approach, for these purposes, is its focus on gathering evidence of relatively defineable crime. So long as illegal conduct is the subject of investigative activity, there is less risk of snooping on legitimate dissenters. But, when security surveillance is divorced from law enforcement, investigations are more likely to involve vaguer, broader, and less defineable matters. This is what could imperil legitimate dissent. In this connection, the American experience becomes instructive. In the mid 1970's, when the Americans confronted the enormity of the civil liberties violations perpetrated by the FBI, they, like us, had to determine a direction which reform ought to take. Instead of creating a civilian security agency divorced from law enforcement, the Americans moved in the diametrically opposite direction. They amalgamated the FBI's domestic security investigations with its general criminal investigative division. The "express purpose" of this move, in the words of the then FBI Director, was to handle domestic security cases as much as possible "like all other criminal cases".<sup>34</sup> In short, the narrower focus of criminal investigations was less likely to intrude on lawful dissent.

This is not necessarily an argument for leaving the security function within the RCMP. Indeed, it appears that the creation of a separate agency may already have become a fait accompli. At this point, we would recommend that the new agency acquire a central law enforcement responsibility for security-related offences. If that were done, Canada would have two federal police forces - one handling security matters, such as espionage, sabotage, and terrorism, and one handling more general criminal investigations such as customs, excise, and drugs. An alternative approach might entail leaving the domestic security work in the RCMP, but like the FBI, integrating it more fully with the criminal investigation branch. If that were done, the new agency would function only in a tightly defined area of counter-intelligence against foreign threats, where the law

enforcement approach might be somewhat more modified. We do not foreclose, of course, on the possibility that there may yet be other acceptable combinations of structures. The essence of our concern is that security surveillance be tied as closely as possible to the discipline of law enforcement.

Recommendation No. 10

- Canada's security functions should not be performed by an all-civilian agency. The activities at issue should be tied more closely to the discipline of law enforcement.

### The Issue of Permissible Law Breaking

Bill C-157 will permit security operatives to break the law when it is "reasonably necessary to enable them to perform" their duties. The government has assured us that this part of the Bill is designed essentially for such minor infractions as automobile speeding and falsely registering in hotels. Unfortunately, however, nowhere does the Bill confine the range of permissible law breaking in that way. It is improbable that many people would mount the barricades to protest the occasional security service violation of some such minor regulatory laws. But there would be considerable distress indeed if the service felt free to violate more serious laws which involved elements of moral turpitude.

In response to these criticisms, the Solicitor General has argued that the test of what is "reasonably necessary" will not be for the security service to decide; it will be subject to scrutiny by the courts. Unfortunately, the Solicitor General has failed to tell us just how the courts are supposed to find out about security service misconduct. While any such law breaking would have to be reported to the federal attorney general, there will be no accompanying obligation either to prosecute, if the matter falls within the federal enforcement jurisdiction, or to relay the information to whatever provincial attorney general may have the prosecutorial authority. The Bill does not even contain restraints on the federal discretion simply to sit on such information. Moreover, another section of the Bill would make it a crime punishable by five years in jail for anyone to disclose any information which could identify a covert security operative. Under such restrictions, how could misconduct be effectively reported?

To whatever extent there is a demonstrated need to grant the security agency relief from complying with certain legal restrictions, the matters at issue should become the subject of specific statutory provisions. Some statutes already provide, for example, that police driving automobiles may exceed the speed limits in certain specified circumstances. There is no reason why similar exemptions could not be enacted in favour of the security and intelligence agency. We are not persuaded by the Solicitor General's aversion to the painstaking exercise that this process might involve. In our view, it

would be infinitely preferable to impose this kind of burden on the parliamentary time table than to inflict the injury on the rule of law which would result so inevitably from the kind of open-ended immunity which Bill C-157 now contains.

Remember too that, even without such immunity provisions, Canadian law already permits a high level of flexibility. Section 27 of the Criminal Code, for example, empowers anyone to use as much force as is reasonably necessary to prevent the commission of a crime which threatens imminently to cause serious harm to persons or property. Our law also preserves the common law defence of necessity under which even otherwise illegal acts may be committed to prevent certain more serious illegal acts when such are imminent.<sup>35</sup> Clearly, the removal of the broad immunity proposed by the government would hardly paralyze our security operations.

While there may be an argument that not every offence committed by a security operative needs to be prosecuted by the federal authorities or reported to their provincial counterparts, we must vigorously oppose the kind of unfettered discretion which Bill C-157 would repose in the federal authorities. If there is to be such a discretion, it should become a matter of discernible guidelines rather than arbitrary preference. And it should become subject to some kind of outside scrutiny. Accordingly, the Bill should be amended to include a set of guidelines to regulate how the government handles evidence of wrongdoing in the security service. An additional amendment should be adopted to provide that, to whatever extent the government may choose against taking action in such a matter, the outside review committee must be immediately notified. The committee should be required to investigate the matter and, at an early date, report its opinion to the government. If a difference of opinion emerged between them, the review committee should be required very shortly to report to Parliament the existence, if not the details, of any such disagreement. The report might even be required to indicate the identity of whatever provincial government might have the requisite enforcement jurisdiction but is being denied the necessary evidence. It is obvious how such a procedure would create political problems for a federal government which decided, in questionable circumstances, to sit on evidence of security wrongdoing.

The Canadian Civil Liberties Association objects strongly to the virtually unqualified prohibition against disclosing any information which could reveal the identity of a covert security operative. Does this mean that victims of illegalities committed by the service may not report them? May they not even tell the police, crown attorney, or M.P.? Are aggrieved citizens to face five years in jail for doing what conscientious citizens are supposed to do - report fully on evidence of suspected illegality?

Such an apparently unadulterated prohibition is unconscionable. Beyond the considerations to which we have referred, the issue also has free speech implications. In our view, the matter would best be left until Parliament deals with the Official Secrets Act. We are prepared to acknowledge that there may be a few particularly contentious areas where the disclosure of information might be so dangerous to the public interest as to justify a legal prohibition. It has generally been conceded, however, that the prohibitions in the Official Secrets Act are perilously broad. Since revisions of that statute have been promised for some time, we would suggest that any contemplated prohibitions on the disclosure of information be deferred so that they might be considered in that context. Surely, the idea must be to narrow as much as possible any prohibitions on the public discussion of public issues. This goal is not likely to be served by the piece-meal accumulation of overbroad prohibitions.

It is not possible to address the misconduct of tomorrow without some consideration to the unfinished business of yesterday. We refer to the refusal of the Canadian Government to apply the normal standards of prosecutorial discretion to all of the evidence of RCMP wrongdoing. In view of the dubious position adopted by the government,<sup>36</sup> how can the Canadian public have the requisite confidence that the misdeeds of the future will be handled more appropriately than the misdeeds of the past? On this basis, we would urge the Committee to recommend a review of the wholesale immunities which the government granted in respect of past RCMP misconduct.

Recommendation No. 11

- To whatever extent there is a demonstrated need to grant the security service relief from certain legal restrictions, the matters at issue should become the subject of specific statutory exemptions rather than a generalized immunity.

Recommendation No. 12

- In response to wrongdoing in the Security Service, guidelines should be enacted specifying the circumstances, if any, under which the government, on security grounds, may exercise a discretion:
  - a) not to prosecute when it has the enforcement jurisdiction and
  - b) not to transmit information when the matter is within the enforcement jurisdiction of a province.

Recommendation No. 13

- The outside review committee should immediately investigate any governmental decision to sit on evidence of security wrongdoing and, to the extent that it differs with such governmental decision, it should report to Parliament the existence, if not the details, of such disagreement.

Recommendation No. 14

- Any proposed prohibitions on the disclosure of information should be deferred until Parliament considers amendments to the Official Secrets Act.

Recommendation No. 15

- There should be a review of the government's decision not to prosecute for the RCMP wrongdoing of the past.

The Issue of Permissible Counteraction

Remarkably, Bill C-157 contains little response to one of the most contentious problems that arose in connection with RCMP wrongdoing. We refer to the many revelations of "dirty tricks". Even if some of these activities could not be attacked on grounds of their illegality, there are serious questions about their acceptability.

It will be remembered, for example, that it was an RCMP officer who had issued the supposed FLQ communique denouncing Pierre Vallieres.<sup>37</sup> Earlier, Mr. Vallieres had publicly renounced terrorism and had urged his followers to join the more moderate and democratic Parti Quebecois. The RCMP officer conceived the fake communique because he feared that an influx of potential terrorists and Marxists would undermine the democratic character of the Quebec separatist party. Since he believed that Vallieres' conversion was not sincere, he felt no moral qualms about any harm that the communique would do to him.

To what extent, however, is it appropriate for a government agency to tamper in this way with the democratic political processes? The RCMP's action could have effectively discouraged support for the democratic Parti Quebecois. While there may have been an element of political sophistication in the officer's judgment, he nevertheless could have been wrong about the sincerity of Vallieres' renunciation of terrorism. To those in the extremist movement who were otherwise susceptible to Vallieres' leadership, the communique could have exerted a harmful influence. In any event, is it the role of a government security service to deny members and supporters, no matter how tenuous their views, to a democratic organization like the Parti Quebecois?

No doubt, such "dirty tricks" found their sustenance in the federal cabinet's 1975 mandate instructing the RCMP security service to maintain internal security "by...detering, preventing, and countering individuals and groups" when their activities fell within the specified criteria. This mandate was embellished in subsequent documents. One internal memorandum, for example, talked about "disruption, coercion, and compromise". In view of the history and supporting materials, how can Bill C-157 say so little about so vital an issue?

The issues have to be more squarely faced. How far is it appropriate for a security agency to foment dissension among targeted constituencies? If not otherwise unlawful, may they compose and circulate fake materials which would appear to have originated with others? To what extent may they resort to deliberate falsehoods in order to mislead and confuse? In short, what options, if any, are available to the security service in addition to merely collecting and reporting on intelligence?

It is not enough for the Bill simply to omit deterring, preventing, and countering from the functions and duties of the security service. Such issues must be handled in explicit terms. Otherwise, there may be an argument that the service is entitled to do whatever it is not prohibited from doing. The Bill should be amended so as to address these questions. It should contain either outright prohibitions or detailed guidelines setting out the permissible limits of what the security service may do to combat whatever security threats it encounters. To whatever extent counteraction is approved, there ought to be considerably less latitude against domestic threats than foreign ones. Again, prosecution will more frequently be the appropriate response in the domestic arena. The history of the past few years has rendered unacceptable any further statutory silence in this area.

Recommendation No. 16

- There should be either outright prohibitions or detailed guidelines setting forth the permissible limits of what the security service may do to combat whatever security threats it encounters.

### Safeguards and Controls

The Canadian Civil Liberties Association appreciates that Bill C-157 will require judicial warrants for the most intrusive surveillance techniques. While such a safeguard is necessary, it is not sufficient. The Bill permits the judge to issue a warrant simply upon being satisfied that it is "required to enable the Service to perform its duties and functions...". As indicated earlier, the use of intrusive surveillance should be accompanied by an ongoing requirement to evaluate security benefits against civil liberties costs. In this connection, the McDonald Commission set out a number of other criteria which the warrant granting judge should consider such as, for example, whether other investigative procedures have been tried and have failed, whether the matter is so urgent that it would be impractical to use other procedures, the value of the intelligence obtained from other warrants in respect of the same investigation etc.<sup>38</sup> The addition of such considerations was designed to limit the granting of warrants as much as possible to those situations where it is really necessary. There is simply no justification for omitting them from Bill C-157. They represent the minimum of what is required.

The McDonald Commission recommended time limits on the survival of judicial warrants.<sup>39</sup> Bill C-157 could conceivably permit lifetime warrants. There is no justification for this either. Time limits ensure that intrusive encroachments will be subjected at least periodically to further independent scrutiny. And, whatever time limits are adopted should distinguish between essentially domestic and foreign-directed threats to the national security. The duration of warrants in the former situation should be considerably shorter than those for the latter.

The Canadian Civil Liberties Association welcomes also the concept of the outside security intelligence review committee. Unfortunately, however, the approach in this area is a flawed one. Members of the review committee will have to be Privy Councillors. As such, they are likely to have an insider's mentality. Moreover, their term of office is only five years. Because it is the government which must decide whether anyone's term will be renewed,

committee members may be tempted to curry favour with the government. At least they will be susceptible to such a perception. Hardly a situation for the kind of independent scrutiny that will command the confidence of the public. And, if all this weren't enough, the Bill expressly provides that the review committee can be denied access to a key source of information about potential government misconduct - confidences of the Queen's Privy Council i.e. cabinet documents.

These flaws should be corrected. The membership of the committee should not be confined to Privy Councillors. The term of office should be more substantially extended and made non-renewable. It should also carry financial benefits sufficient to enable the members to live comfortably after their terms of office. In that way, there will be less incentive for any member to curry favour with the government. Moreover, the committee should have access to everything relevant in the possession of the security service and the government including confidences of the Queen's Privy Council. Complete access is the prerequisite of public confidence.

We are concerned also about the risk that, even with these changes, the review committee will increasingly identify with the security service. This has often been the case in the relationship between regulatory agencies and the businesses they had to regulate. In these circumstances the risk has to be compounded because of the secrecy which will characterize the relationship. In this regard, the McDonald Commission made a most useful recommendation that an additional oversight role be played by a small parliamentary committee composed partly of opposition members. The introduction of such a perspective could help to reduce the risks of an excessively cozy relationship. We believe that the Bill should be amended so as to implement this recommendation.

Even if the review committee were to identify improprieties in the security operations, what could be done about them? Under the Bill, the minister will not be able to override the director of the service on any question about the surveillance of particular persons or groups. How, then, could the minister exercise the requisite supervision and control? His power to issue general directives would likely be too little; his power to discharge

the director could well prove too much. To be properly accountable, the minister must be able to step in and simply say "no" to the dubious practices he encounters. Significantly, the McDonald Commission called for the exercise of such ministerial power over security operations. In this regard, the Commission noted how much more political judgement is involved in security operations than in regular police work. On this basis, we believe the minister should be given such additional control.

Recommendation No. 17

- The courts granting warrants for intrusive surveillance should be guided at least by the additional criteria recommended by the McDonald Commission.

Recommendation No. 18

- There should be statutory time limits for the duration of such warrants, considerably shorter in the case of domestic threats than foreign ones.

Recommendation No. 19

- As regards the outside review committee, the following changes should be made:
  - a) the membership should not be confined to Privy Councillors
  - b) the term of office should be substantially extended and made non renewable
  - c) there should be financial benefits sufficient to enable the members to live comfortably after their term of office
  - d) there should be access to everything relevant in the possession of the security service and the government including confidences of the Queen's Privy Council.

Recommendation No. 20

- An additional oversight role should be played by a small parliamentary committee composed partly of opposition members.

Recommendation No. 21

- The minister should be given greater control over operational decisions.

Recommendation No. 5

- The security and intelligence agency should have no investigative access to census and income tax information relating to citizens and permanent residents. The agency's special access to all other such personal information in government data banks should require, at the very least, reasonable grounds to suspect a serious security-related breach of the law.

Recommendation No. 6

- The governing statute should contain provisions specifying the circumstances under which informants may be deployed and the officials who must approve such deployment.

Recommendation No. 7

- The statute should also contain guidelines regulating informant behaviour during such undercover operations.

Recommendation No. 8

- While the targeting of foreign visitors and the use of less intrusive techniques might be permitted on the basis of lower standards, the governing statute should nevertheless spell out both the applicable standards and the level of official who should be empowered to authorize the requisite techniques in the circumstances at issue.

Recommendation No. 9

- There should be more specific criteria governing the retention, disclosure, and destruction of surveillance material. Such criteria should also address how the material is to be stored, who should have access to it, and how such access should be facilitated.

Recommendation No. 10

- Canada's security functions should not be performed by an all-civilian agency. The activities at issue should be tied more closely to the discipline of law enforcement.

Recommendation No. 11

- To whatever extent there is a demonstrated need to grant the security service relief from certain legal restrictions, the matters at issue should become the subject of specific statutory exemptions rather than a generalized immunity.

Recommendation No. 12

- In response to wrongdoing in the Security Service, guidelines should be enacted specifying the circumstances, if any, under which the government, on security grounds, may exercise a discretion:
  - a) not to prosecute when it has the enforcement jurisdiction and
  - b) not to transmit information when the matter is within the enforcement jurisdiction of a province.

Recommendation No. 13

- The outside review committee should immediately investigate any governmental decision to sit on evidence of security wrongdoing and, to the extent that it differs with such governmental decision, it should report to Parliament the existence, if not the details, of such disagreement.

Recommendation No. 14

- Any proposed prohibitions on the disclosure of information should be deferred until Parliament considers amendments to the Official Secrets Act.

Recommendation No. 15

- There should be a review of the government's decision not to prosecute for the RCMP wrongdoing of the past.

Recommendation No. 16

- There should be either outright prohibitions or detailed guidelines setting forth the permissible limits of what the security service may do to combat whatever security threats it encounters.

Recommendation No. 17

- The courts granting warrants for intrusive surveillance should be guided at least by the additional criteria recommended by the McDonald Commission.

Recommendation No. 18

- There should be statutory time limits for the duration of such warrants, considerably shorter in the case of domestic threats than foreign ones.

Recommendation No. 19

- As regards the outside review committee, the following changes should be made:
  - a) the membership should not be confined to Privy Councillors
  - b) the term of office should be substantially extended and made non renewable
  - c) there should be financial benefits sufficient to enable the members to live comfortably after their term of office
  - d) there should be access to everything relevant in the possession of the security service and the government including confidences of the Queen's Privy Council.

Recommendation No. 20

- An additional oversight role should be played by a small parliamentary committee composed partly of opposition members.

Recommendation No. 21

- The minister should be given greater control over operational decisions.

NOTES

1. U.S., Congress, Senate, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Report No.94-755, 94th Congress, 2d Session, 1976, Book II, p.19.
2. Ibid.
3. Ibid., p.359.
4. Ibid., p.19.
5. Richard, Eric. "Unleashing the Intelligence Community", 69 American Bar Association Journal 907 at 908.
6. In the case of United States v. United States District Court 407 U.S. 297 (1972), the Supreme Court of the United States held there is no executive power to authorize electronic surveillance against domestic security threats without prior judicial approval. While the Court indicated that it might be open to the U.S. Congress to create a bugging power for domestic security purposes which is broader than what is available for criminal law purposes, no such legislation has ever been passed or sought. Since this case, all electronic bugging against domestic security threats has been conducted under the Omnibus Crime Control and Safe Streets Act, Title 3, 18 U.S.C. § 2516.
7. Foreign Intelligence Surveillance Act, Title 50, 30 U.S.C. §1801.
8. Nor would we object to activating any of the named surveillance techniques, subject to proper safeguards, in order to rescue human life or limb in a situation of imminent peril.
9. Schwartz, Herman, "Reflections on Six Years of Legitimated Electronic Surveillance", Privacy in a Free Society (Boston, Mass: Roscoe Pound-American Trial Lawyers Foundation, 1974), pp.47, 48.
10. Schwartz, Herman, "A Report on the Costs and Benefits of Electronic Surveillance-1972", ACLU Report, March, 1973.
11. U.S., Report of the National Commission For The Review Of Federal And State Laws Relating To Wiretapping And Electronic Surveillance, Washington, 1976, p.4.
12. Schwartz, Herman, Taps, Bugs, and Fooling the People (Published by The Field Foundation, 100 East 85th Street, New York, N.Y., June 1977), p.38.
13. Canada, Parliament, Report of Solicitor General, Annual Report as Required by Section178.22 of the Criminal Code, 1978.
14. Canada, Parliament, Report of Solicitor General, Annual Report as Required by Section16(5) of the Official Secrets Act, 1978.
15. U.S., Congress, Senate, Select Committee on Intelligence, Electronic Surveillance Within the United States For Foreign Intelligence Purposes, Hearings before the Subcommittee on Intelligence and the Rights of Americans, 94th Cong., 2nd Sess., p.113.
16. Supra, fn.12, p.39.
17. Elliff, John T., The Reform of FBI Intelligence Operations (Princeton, New Jersey: Princeton University Press, 1979), p.41.
18. Supra, fn. 12, p.40.
19. Ibid, p.39.
20. The Criminal Code, R.S.C. 1970, Chap.C-34, s.178.1.
21. Ibid. Bugging under the Criminal Code contemplates, of course, a law enforcement rather than an intelligence gathering purpose. See also Elliff, supra, fn.17, p.159.

22. Foreign Agents Registration Act, Title 22, 11 U.S.C. § 611.
23. Supra, fn. 6.
24. Supra, fn. 7.
25. Supra, fn. 6, § 2516 and 2518.
26. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Freedom and Security Under the Law Second Report Volume 1 (Ottawa: Queen's Printers, 1981) at 575.
27. Section 8(2)(e) of the Privacy Act allows information disclosures, without warrant, to investigative agencies. In a letter to the Government, dated May 20, 1982, CCLA made the following complaint about this section. "It is rare when the law permits investigative agencies to invade residential privacy without a judicial warrant. Yet Bill C-43 permits these agencies to invade informational privacy without any semblance of such a safeguard. You will appreciate, therefore, the wholesale snooping which could result. It is significant that the report of the McDonald Commission also criticized the potential for abuse which this section would create".
28. Supra, fn.26, p.587.
29. First Principles, published by Project on National Security and Civil Liberties, March 1977, Vol.2, Number 7, p.4.
30. Ibid, p.3.
31. Hoffa v. U.S. 385 U.S. (1966), p.302.
32. Ira S. Shapiro, "The Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and the Fourth Amendment", 15:1 Harvard Journal on Legislation 119 at p.173.
33. Regrettably, even the McDonald Commission rejected this distinction between residents and visitors. Supra fn.26, p.580.
34. Supra, fn. 17., p.190.
35. See Criminal Law by Mewett & Manning (Toronto: Butterworths, 1978), p.305: "It is suggested that, on the very few authorities that are available, the defence of necessity does now exist in Canada and that the limitations are as follows. Where an accused believes upon reasonable and probable grounds that serious harm will befall himself or some other person, he is justified in committing a criminal offence to avert that harm if there is such an emergency that no other course of conduct is reasonably possible in order to prevent that harm; but this defence does not apply where the offence committed gives rise to more serious harm that sought to be prevented."
36. For a point by point response to the government's defence of its no-prosecution policy see Borovoy, A. Alan, "Ottawa Shirks Its Duty To Prosecute RCMP Wrongdoers," Toronto Star, 12 February 1983.
37. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. Proceedings, vol. 65, pp. 10593-10643.
38. Supra, fn. 26, p. 596.
39. Supra, fn. 26, p. 596.