SUBMISSIONS TO - Special Committee on the Review
of
The Canadian Security Intelligence Service (CSIS) Act
House of Commons

RE - The Five-Year Review

FROM - Canadian Civil Liberties Association

DELEGATION - A. Alan Borovoy
(General Counsel)

Kenneth P. Swan
(Vice-President & Chairman of the Board)

Catherine Gilbert
(Research Director)

Ottawa January 16, 1990

Contents

Contents

Introduction

The Canadian Civil Liberties Association is a national organization with more than 7000 paid individual supporters, seven affiliated chapters across the country, and some 50 associated group members which themselves represent several additional thousands of people. A wide variety of persons and occupations is represented in the ranks of our membership - lawyers, academics, homemakers, trade unionists, journalists, clergy, 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 the CSIS Act. In crucial respects, the Act could permit substantial encroachments upon the fundamental freedoms of the individual.

One of the most obvious of these imperilled freedoms is personal privacy. To the extent that information about us passes beyond our control, our sphere of personal privacy is reduced. So often we hear the admonition, "if you have nothing to hide, why worry". Those who have nothing to hide are probably leading very dull lives. The issue, of course, goes deeper. Merely to pose such questions is to treat people as though they were nothing more than what former Ontario Chief Justice J.C. McRuer called,

"micro-organisms of the state". Personal privacy is a component of human dignity. The question is not what have we to hide but what is the justification for the intrusion on us.

Security intelligence surveillance is also a threat to political liberty. An essential component of the concept of self-government is the right to dissent -- to speak, write, publish, assemble, associate, and organize freely and openly in opposition to incumbent governments and their policies. To the extent that security intelligence investigations have a political component (and they almost always have), they could intimidate the exercise of these liberties. For many people, the knowledge or even the suspicion that government agents are secretly watching may be sufficient to deter their participation in political dissent. The democratic system cannot viably function in such a chilled atmosphere.

Nevertheless, in the troubled and dangerous world of today, we do not, indeed we cannot, object to the existence of a special agency to perform security and intelligence functions. It is not yet clear to what extent the traditional pattern of Soviet expansionism has been irreversibly moderated by the upheavals in the Eastern Bloc. But, even if the Communist world has undergone permanent change in this regard, the persisting existence of 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.

On the other hand, the endorsement of the goal does not carry with it 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.

Since the introduction of the CSIS legislation into the House of Commons, the Canadian Civil Liberties Association has expressed serious criticism of its provisions. We believe that the powers are excessive and the safeguards are inadequate. Overbroad definitions of what constitutes a threat to the security of Canada can trigger a host of intrusive powers of surveillance. Little 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 try in a number of situations to recommend specific alternatives. In view of the enormity of the issue, however, we shall focus on some issues in greater detail than on others. At this point, our primary concern is the scope of intrusive surveillance that is available against Canadian citizens and permanent residents. By this, we mean electronic bugging, surreptitious searches, mail opening in

the course of post, the invasion of confidential records, and the deployment of covert informants. Of course, our organization is also concerned about less intrusive forms of surveillance and the scope of protections for foreign visitors. But more detailed recommendations on these matters, as well as the issue of security clearances, will have to await our efforts to seek reform in the areas of our more urgent interest.

Since our brief is addressed only to the 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 powers should be no greater than the general law enforcement powers. 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 to explore the ambit of the regular criminal law. The fulfilment of that objective will continue to occupy us in other contexts.

The First Five Years

Following the recommendations of two royal commissions (MacKenzie and McDonald), the Canadian Security Intelligence Service (CSIS) was created as a civilian agency with no law enforcement functions. Its mandate is to engage in preventive intelligence gathering in respect of threats to Canada's national security. It was hoped that a civilian agency would be more likely than a

police agency to avoid the kind of improprieties and civil liberties violations that had stained the record of the RCMP Security Service.

But a mere three years after the birth of CSIS, it too became engulfed in hot water.

*The first CSIS director resigned because of the revelation in a British Columbia court that CSIS had used improper material for a wiretap warrant it had obtained during its investigation of the June 1985 Air India plane disaster.[1]
*A CSIS informant pleaded guilty in a Quebec court to participation in the planting of bombs during a labour dispute involving a union he had infiltrated.[2]
*The Security Intelligence Review Committee (SIRC), the watchdog created by Parliament to monitor security activities, criticized CSIS for "intruding on the lives and activities of too many Canadians"; in SIRC's view, "CSIS over-estimates the likelihood of violence by some groups".[3]

Since the publication of SIRC's 1986-1987 report, this situation has apparently improved. CSIS' counter-subversion branch has been abolished. According to SIRC, the number of questionable CSIS investigations has significantly declined. Indeed, SIRC's 1987-1988 report expresses the hope that CSIS has finally "turned the corner" on some of its earlier dubious practices.[4]

But, despite these signs of progress, there are indications that serious problems persist. As recently as the spring of 1989, the Canadian Civil Liberties Association obtained affidavits in which the deponents accused CSIS of meddling in the affairs of legitimate protest organizations. One involved a refugee aid group in Alberta and another involved a trade union in British Columbia.[5] In the spring of 1989, there were newspaper reports that CSIS had been conducting some questionable investigations of

the Innu in Labrador.[6] And, even in the midst of acknowledging improvement, SIRC's 1987-1988 report criticized the magnitude of a particular CSIS operation.[7] While noting a significant reduction in this and other dubious investigations in its 1988-1989 report, SIRC declared that it still has "concerns" about certain CSIS practices such as those relating to the peace movement.[8]

In fairness, it may not be possible to eliminate all of the tensions between the requirements of security and the interests of civil liberties. Some proclivity to take questionable short cuts may be endemic to the very nature of a national security operation. But, no matter how inevitable we believe these problems to be, we must try to deal with them. To fail even to make an effort is to suffer the erosion, sooner or later, of our democratic institutions.

Intrusive Surveillance of Citizens and Residents

One of the central problems is the breadth of powers available to CSIS under the Act. Inevitably, statutory power sends signals to those who are called upon to exercise it -- in this way, excessive power tends to legitimate excessive use.

The statutory powers are currently so broad that Canadian citizens and permanent residents are lawfully vulnerable to electronic bugging, surreptitious searches, mail opening, the invasion of their confidential records, and the deployment of covert informants even when there isn't the slightest suggestion of any illegality -

or, indeed, the slightest threat to our national security.

By virtue of section 2(b) and other provisions, such intrusive surveillance can be used to monitor "foreign influenced activities...that are detrimental to the interests of Canada and are clandestine or deceptive...". "Influence" covers a lot of territory. If the Canadian Civil Liberties Association draws inspiration from the American Civil Liberties Union, does this mean that CCLA is "foreign influenced"? What are the limits of "detrimental"? Suppose certain Canadian citizens were employed by a foreign corporation 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"? Could those serving such interests have their conversations bugged, premises searched, mail opened, and records invaded? The requirement that the targeted activities be "clandestine or deceptive" may not adequately diminish the danger. There is an element of the "deceptive" in many commercial transactions.

In combination with other provisions, section 2(c) of the Act potentially entitles CSIS to use all of these intrusive surveillance techniques to monitor "...activities...directed toward or in support of...acts of serious violence...for the purpose of achieving a political objective within Canada or a foreign state...". Those words are broad enough to have permitted such eavesdropping on Canadian citizens who raised money for the state of Israel following the Yom Kippur invasion. It could similarly

imperil those who send financial help to the rebels in El Salvador, Namibia, or the contras in Nicaragua. Even if such "activities" are lawful, open, and free of foreign control, the law makes those who conduct them potentially vulnerable.

Under section 2(d), CSIS is mandated to probe, inter alia, "activities...intended ultimately to lead to the destruction or overthrow by violence, of the constitutionally established system of government in Canada". How are CSIS operatives supposed to get evidence of "ultimate" intentions? Can the word "ultimately" deal with any point between now and the end of time? It is obvious that this language could encourage speculation about the hereafter, rather than evidence from the here and now, to serve as the prerequisite for surveillance. These words could well encourage CSIS to make extravagant predictions of future violence. The problem is the more speculative the exercise becomes, the greater the risk of intruding on completely lawful behaviour. It is dangerously improper, therefore, to allow this sub-section to serve as a mandate for electronic bugging, surreptitious searches, mail opening, the invasion of confidential records, and the deployment of covert informants.

Moreover, there are real doubts whether the dangers created by section 2 are sufficiently diminished by the subsequent exemption for "lawful advocacy, protest or dissent".[9] It is not clear if lawful activities such as fund-raising or commercial negotiations would be covered by this exemption.

Nor can we derive significant consolation from the fact that

some of the most intrusive surveillance techniques require prior judicial authorization.[10] The judges are not asked to determine whether they consider the circumstances at issue a genuine threat to Canada's security. Rather, their role is essentially to determine whether those circumstances fall within the statutory criteria for permissible surveillance. If the statutory criteria are too vague and broad, we cannot rely on the need for judicial warrants to rescue us from excessive surveillance. Remember too that one of the intrusive surveillance techniques - the deployment of covert informants - does not require judicial warrants.

With such vague and broad powers that exceed any genuine security threat, it is not surprising to learn that SIRC has "concerns" about certain CSIS proclivities. The breadth of its surveillance mandate virtually invites CSIS to spy excessively.

Nor is this to overlook the action taken in late 1987 by former Solicitor General James Kelleher on the recommendation of a special committee he had established to review SIRC's damaging report. To his credit, Kelleher abolished the counter-subversion branch that CSIS had been operating. This branch had been the one involved in much of the dubious surveillance. While we should welcome Mr. Kelleher's action, we must also question whether it goes far enough. Even if this branch no longer exists, the powers that it had remain available to CSIS as a whole. It is important, therefore, to examine not only the details of certain operations but also the central philosophy from which they spring.

At base, it is difficult to square these surveillance powers 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 believe that certain criminal offences are involved. 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 the slightest suggestion that the law is being violated?

We will be told, of course, that the special role of security intelligence is to prevent the apprehended harms before the country suffers them.[11] As attractive as this approach might appear, the dangers must be appreciated. A broadly preventive mandate 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 and non-threatening conduct.

Moreover, there is good reason to question how much additional security is obtained through this level of 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".[12] In 1974, for example, the GAO estimated that the FBI obtained advance knowledge of its targets' activities in only about 2% of all its investigations. And most of this knowledge related to completely lawful activities such as speeches, meetings, and peaceful demonstrations.[13] 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".[14] 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 1960s.[15]

Accordingly, American law-makers have adopted a number of measures to restrict the scope of the FBI's preventive intelligence gathering. 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 actual crimes are involved.[16] 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.[17] 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.[18]

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 sitiuations, 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 the CSIS Act.

In our view, the best solution would be to require that citizens and permanent residents not be targetable for intrusive surveillance unless, at the very least, there are reasonable grounds to believe that the matter under investigation involves a serious security-related breach of the law such as espionage, sabotage, serious violence, extortion, or bribery impairing the operations of government. Since law-breaking involves not only completed acts, but also attempts, counselling, aiding, abetting, and even conspiracies, this should afford enough preventive scope to the intelligence-gathering exercise. Indeed, there is considerable risk that the inclusion of conspiracies could still cast too wide a net. Perhaps, for such purposes, intrusive surveillance should require evidence not only of a conspiracy but also of some overt conduct in furtherance of it.

While some forms of intrusive surveillance against citizens and permanent residents should require even additional conditions, none should be allowed on the basis of anything less.

Recommendation No. 1

Citizens and permanent residents should not be targeted for electronic bugging, mail opening, surreptitious entry, invasion of confidential records, or the deployment of covert informants unless, at the very least, there are reasonable grounds to believe that the matter under investigation involves a serious security-related breach of the law such as sabotage, espionage, serious violence, extortion, or bribery impairing the operations of government.

While some of these intrusive techniques should require even more exacting standards, none should be allowed on the basis of anything less.[19]

The Special Problem of 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, informants not only spy but they also participate. If they are sufficiently charismatic, they can effectively distort the political activities of the groups they infiltrate. Indeed, they might even provoke some of the very illegalities which they have been assigned to detect.

Apart from professional undercover agents, informants are often unstable and disreputable people. In this connection, it is interesting to note that the attempted assassin of former President Gerald Ford was an FBI informant.[20] 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.[21]

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, the CSIS Act is remarkably devoid of attempts to regulate the activities of the 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".[22] There is, of course, some truth in this. Unlike bugs and physical searches, there is some control over whom we 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 the Act 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 at once is 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 informants might distort, exaggerate, and perhaps even fabricate in order to enhance their 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 regulate security and intelligence activity 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. 2

The governing statute should contain provisions specifying:
a) the officials who must approve the deployment of covert informants and
b) guidelines for regulating the behaviour of such informants during undercover operations.

Either/Or Choices

There is a basic flaw in the structure of the CSIS Act. Under the current provisions, subject matters are either completely inside or completely outside of the CSIS mandate. Anything within the mandate is capable of authorizing the most intrusive investigative techniques. Conversely, anything outside of the mandate might not even arguably be the subject of study from open and public sources.

Suppose, for example, CSIS relied entirely on open sources to

inform itself of background trends and developments in our society? On CSIS's part, this might entail clipping and storing items from the press, promoting seminars and discussions, and inviting experts to lecture its operatives. It might be very difficult to criticize CSIS for engaging in such an information-gathering exercise. Unfortunately, the present structure of the Act forces Canadians to choose between allowing section 2 to mandate virtually everything conceivable or nothing imagineable. In our view, there is no need to confront such a dilemma.

Indeed, even where actual targeting is concerned, there may be an argument for lowering the standards as the magnitude of intrusiveness decreases. While watching, trailing, interviewing, and source checking are intrusive, they are nowhere near as intrusive as electronic bugging, surreptitious searches, mail opening, the invasion of confidential records, and the deployment of covert informants. In any event, the statute should make distinctions in the circumstances that must apply for more and less intrusive techniques of information-gathering -- the more intrusive the technique , the more demanding the tests for authorizing it.

The way the Act is currently structured, citizens, permanent residents, and temporary visitors are, with few exceptions, treated alike. If their "activities" fall within any of the definitions in section 2, they can be targeted for the most intrusive surveillance. Otherwise, it is possible that they cannot be considered a fit subject for any kind of CSIS attention.

In our view, the legal status of a proposed target should

influence the intrusiveness of the surveillance that might be used. Surely, 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. Visitors could well be here for only brief periods - weeks or perhaps even days. That might not afford enough time for our security agents to acquire the kind of preliminary evidence that should be required for intrusive surveillance of citizens and permanent residents. Moreover, experience indicates that, compared with citizens and residents, a significantly higher proportion of visitors is involved in foreign intelligence activity.[23]

It is important to resist the tantalizing arguments of those who urge a false egalitarianism. Some have suggested, for example, that it is unfair to make distinctions between residents and visitors. Their solution is to propose low standards for everyone. Such an argument was advanced, for example, by the senate committee that made recommendations on the government's first national security bill (C-157).[24] Yet the committee did not abide by its own argument. Its report proposed that citizens and permanent residents be exempted as targets for the collection of certain intelligence relating to the activities of foreign states.[25]

influence the intrusiveness of the surveillance that might be used. Surely, 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. Visitors could well be here for only brief periods - weeks or perhaps even days. That might not afford enough time for our security agents to acquire the kind of preliminary evidence that should be required for intrusive surveillance of citizens and permanent residents. Moreover, experience indicates that, compared with citizens and residents, a significantly higher proportion of visitors is involved in foreign intelligence activity.[23]

It is important to resist the tantalizing arguments of those who urge a false egalitarianism. Some have suggested, for example, that it is unfair to make distinctions between residents and visitors. Their solution is to propose low standards for everyone. Such an argument was advanced, for example, by the senate committee that made recommendations on the government's first national security bill (C-157).[24] Yet the committee did not abide by its own argument. Its report proposed that citizens and permanent residents be exempted as targets for the collection of certain intelligence relating to the activities of foreign states.[25]

Recommendation No. 3

The Act should be restructured so as to require more demanding tests in order to authorize

a) more intrusive over less intrusive techniques of information-gathering and
b) the surveillance of citizens and permanent residents over the surveillance of visitors.

Civilianization

In the opinion of the Canadian Civil Liberties Association, not enough attention has been paid to the role civilianization itself has played in certain dubious activities of CSIS. A law enforcement agency would be less likely than a purely intelligence-gathering agency to employ the kind of improper materials that characterized the CSIS wiretap warrant applications in the Air India case. Law enforcement agencies must anticipate intense scrutiny of their material by partisan defence counsel in open court. No one would expect comparably rough treatment by impartial judges at the in camera hearings for warrant applications. The defence lawyer would be trying to discredit the agency's material; the judge would simply be reviewing it. Moreover, the defence counsel would likely know a lot more about the case than would a judge. Thus, the anticipated use of material for subsequent prosecutions would help to restrain the investigators from engaging in conduct that would undermine their case.

The same could well apply also to the CSIS informant who was involved in the bomb conspiracy during the Quebec labour dispute. Had CSIS been using this informant in order to acquire evidence

for a prosecution, it might have been far more careful to ensure that there would be no embarrassing disclosures. Note that SIRC specifically criticized CSIS for its insensitivity to this man's "potential...to become involved in illegal activities".[26] The problem is that intelligence gathering unrelated to a prosecutorial outcome is less likely to be concerned about the appearance of propriety. In short, the agency does not as readily expect to be found out.

This is not to say, of course, that such improprieties do not occur within the framework of law enforcement operations. Obviously, they have. Our point simply is that, as between a law enforcement and an intelligence gathering operation, the latter is more likely to attract such troubles because it has less incentive to avoid them.

The propensity to engage in excessive investigations is also a concomitant of civilianization. A civilian agency does not make policy or enforce the law; its main function is simply to gather intelligence. Since the goal of an intelligence investigation is to assess, understand, and predict, the idea is to learn as much as possible. Hence, the tendency to investigate an excessive number of people. Moreover, the idea is to discover almost everything there is to know about the targets, including their most intimate habits and beliefs. Hence, the tendency to investigate an excessive number of activities.

The problem is that it is very difficult to conduct such pervasive surveillance without casting a chill over political

liberty and personal privacy. At the very least, many people are likely to feel that they are under surveillance. This will particularly apply to those who have unconventional opinions and ideologies. If such people think their organizations are infested with spies, they will not speak freely at their meetings. If they think they are being followed, they will not attend certain functions. Thus, there could be a substantial reduction in their enjoyment of their fundamental freedoms. A viable state of civil liberties requires not only the reality of their existence, but also the experience of their enjoyment.

By contrast to an intelligence investigation, a law enforcement investigation is a more limited exercise. It is designed - essentially to collect evidence for the purpose of prosecution. Its scope is limited to gathering evidence of crime; its duration is limited to the period before trial. As a consequence, the law enforcement investigation is much less threatening to civil liberties.

The further 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 definable 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

definable matters. This is what could imperil legitimate dissent.

Significantly, the revelations of the abuses committed by the American FBI impelled the US authorities to move in the diametrically opposite direction from what was done in Canada. Instead of creating a civilian security agency divorced from law enforcement, the Americans 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 investigations as much as possible "like all other criminal cases".[27] The narrower focus of criminal investigations was seen as less likely to intrude on lawful dissent.

While trouble may be inherent in the very nature of security and intelligence operations, it is noteworthy that the security intelligence activities of the FBI were relatively scandal-free for about seven years after the reforms of the early and mid-1970s. Even at that, the scandal that did surface - the CISPES investigation - has been characterized by the Senate Intelligence Committee as essentially an "aberration".[28] By comparison, the problems plaguing CSIS appear to have existed almost from the time the agency was created. This contrast becomes all the more striking when we consider that, because of America's pivotal position in the world, its intelligence agencies must have been under much more intense pressure than their Canadian counterparts to employ dubious tactics. All of these considerations prompt us to recommend that Canada move intelligence collection and law

enforcement closer together rather than farther apart.

We appreciate the fact that not every investigation can have a prosecutorial outcome or even purpose. Quite often, for example, foreign espionage is more effectively counteracted without resort to criminal trials which risk the exposure of confidential sources and material. But, whatever need there may be for flexibility, the security intelligence agency should have law enforcement as well as intelligence collection functions. Even if there is often a need to focus on tactics other than prosecution, the fact that the agency may have to prosecute at some stage could diminish some of its propensities to take questionable short cuts.

Housing law enforcement and intelligence collection in the same agency also helps to reduce some of the conflicts that characterize inter-agency relations. A few months ago, for example, the Canadian public learned of an operation entitled the National Security Investigations Section (NSIS).[29] This is a division within the RCMP. Apparently, NSIS engages in a certain amount of preventive intelligence investigation of security matters. The tendency to do this must be virtually irresistable. In all fairness, how can this country expect the RCMP to enforce the law in certain national security areas without allowing it to engage in any intelligence information gathering in relation to its mandate? It is very difficult to encumber an agency with certain duties and then expect that agency to rely on others for the information that would facilitate the discharge of those duties.

Accordingly, the Canadian Civil Liberties Association recommends that law enforcement be added to the functions of those who are involved in security intelligence. This could be done in different ways. Perhaps, for example, CSIS might acquire law enforcement duties 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 regular criminal investigations relating to such areas as customs, excise, and drug violations. An alternative approach might entail leaving the domestic security work within the RCMP, but, like the situation with the FBI, integrating it more fully with the criminal investigation branch. If that were done, CSIS would function only in a tightly defined area of counter-intelligence against foreign-controlled security threats. In such event, the activities of SIRC would have to be extended to cover the RCMP. No doubt there are additional structures that will acomplish the same objective. We are not now wedded to any one solution. Our point simply is that the collection of security intelligence no longer be divorced from the job of law enforcement.

Recommendation No. 4
The agency primarily charged with the collection of security intelligence should also have law enforcement duties with respect to the same matters.

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".[30]

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 the CSIS Act 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 the Act 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.

Since computers render everything instantly retrievable, it would be helpful also for the 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. 5

There should be specific criteria governing the retention 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.

Counteraction

Remarkably, the CSIS Act contains little response to 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 the 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.[31] 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 believed that Vallieres' conversion was insincere and he feared that an influx of potential terrorists and Marxists would undermine the democratic character of the Quebec separatist party.[32] Accordingly, the officer suffered no apparent qualms about what he had done; indeed, he said he would consider doing it again.[33]

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, the "dirty tricks" found their sustenance in the federal cabinet's 1974 mandate instructing the RCMP security service to maintain internal security "by...deterring, preventing, and countering individuals and groups"[34] 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".[35] In view of the history and supporting materials, how can the Act 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 the agency compose and circulate fake materials which would appear to have originated with others? To what extent may it 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 Act simply to omit deterring, preventing, and countering from the functions and duties of the security agency. Such issues must be handled in explicit terms. Otherwise, there may be an argument that the agency is entitled to do whatever it is not prohibited from doing. The Act 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 agency 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. 6

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

Safeguards and Review Mechanisms

The Canadian Civil Liberties Association welcomes the role and performance of the Security Intelligence Review Committee (SIRC). The reports of this committee have given the public a useful "window" on the secret activities of CSIS. Nevertheless, some reforms are in order.

The current term of a SIRC member is only five years. And, since the government must decide whether or not to renew any of the incumbents' terms of office, committee members may be tempted to curry favour with the government. In any event, the committee members might become susceptible to such a perception. At some point, this could undermine public confidence in the operation. In order to reduce the possibility of such perceptions, the SIRC term of office should be substantially extended and made non-renewable.

At the moment, the Act expressly provides that SIRC can be denied access to a key source of information about potential CSIS misconduct - confidences of the Queen's Privy Council i.e. cabinet documents. There is no excuse to shut SIRC out in this way. It should have access to everything relevant in the possession of CSIS

and the government, including cabinet documents. Complete access is the prerequisite of public confidence.

Also, the Act currently contains no protection for CSIS members who report possible acts of wrongdoing to SIRC. Indeed, such complaints must first be lodged with the CSIS director. It is conceivable that this combination of loophole and requirement could effectively deter CSIS members from exposing misconduct. The Act should be amended in order to ensure that CSIS "whistle- blowers" can go directly to SIRC and enjoy immunity from identification and discipline.[36]

Periodically, we hear reports that governmental operations outside of CSIS are involved in security intelligence activity - the mysterious CSE, the military, external affairs, and, of course, the RCMP. The resulting situation is inexplicably inconsistent. Why should CSIS be the only government security operation that is made subject to the scrutiny of SIRC? To what extent are other departments being allowed to commit unaccountable misdeeds? Again, no matter what the facts are, the public perception is bound to be one of deep suspicion. Accordingly, CCLA recommends that the jurisdiction of SIRC be extended to all government operations that are involved in security intelligence activity.

We are also concerned about the risk that, even with these changes, SIRC might come increasingly to identify with CSIS. This has often been the case in the relationship between regulatory agencies and the businesses they had to regulate. In

these circumstances, the risk is compounded because of the secrecy which characterizes 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 this perspective could help to reduce the risks of an excessively cozy relationship, or at least the perception of such a relationship.

One of the most important safeguards that can be brought to play in respect of any government operation is vigorous scrutiny by Parliament. The vigor of such scrutiny must depend, of course, upon the M.P.s themselves. While statutory provisions cannot guarantee how Parliament actually behaves, they can create the opportunity for the kind of scrutiny that is needed. For these reasons, we are grateful that the 1984 CSIS Act provided for a five year review by Parliament. In view of the potential perils to civil liberties inherent in such legislation, the Canadian Civil Liberties Association believes that the Act should provide for automatic five-year reviews by Parliament in perpetuity.

Recommendation No. 7

As regards SIRC, the following changes should be made:
a) the term of office should be substantially extended and made non-renewable
b) there should be access to everything relevant in the possession of CSIS and the government, including confidences of the Queen's Privy Council
c) whistle-blowers should be able to complain directly to SIRC and they should be granted immunity from identification and, if necessary, from discipline
d) SIRC's jurisdiction should extend to every

governmental operation involved in security intelligence activity.

Recommendation No. 8

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

Recommendation No. 9

There should be automatic reviews of the statute by Parliament every five years.

APPENDIX

A Partial Response to the SIRC Recommendations

effective sovereignty i.e. its self-determination, would thereby be diminished? In this way, the SIRC definition might be capable of authorizing the intrusive surveillance of Canadian citizens in commercial situations that raised no security threats whatsoever.

Another illustration might also be helpful. Suppose a Canadian citizen, openly employed by the World Council of Churches, joined the local peace movement and began to agitate for Canadian military disarmament? And suppose this citizen, in order to be credible, claimed to believe that the West should disarm only if the Soviet Union did but, in fact, his religious philosophy required his potential support for unilateral disarmament by the West? To the extent that this person was employed by the World Council of Churches, we might designate his activities as "foreign directed". To the extent that he pretended to be closer to the mainstream of Canadian political thinking than he really was, his activities might be described as "deceptive". And, to the extent that his activities might lead to the reduction of our armaments, they might be seen as "weakening Canada's military defences". On the basis of the SIRC proposal, therefore, this Canadian citizen might be vulnerable to intrusive surveillance by CSIS. Yet he could hardly be considered a genuine threat to the security of Canada.

In the absence of serious security-related law-breaking, why should Canadian citizens and permanent residents be vulnerable to intrusive surveillance because of their various agency relationships with foreign powers? According to the McDonald

Commission, the underhanded tactics by which foreign agents have attempted to influence Canadian life have included threatening reprisals against the overseas relatives of ethnic leaders in this country, compromising politicians or government officials under threats of blackmail, attempting to acquire scientific information for the benefit of our international trade competitors, and the clandestine employment of Canadian government officials to support the interests of certain foreign governments. The Commission also talked about the secret funding by foreign governments of voluntary activity in Canada.[37]

By and large, most of these impugned tactics constitute offences under Canadian law. Consider, for example, the prohibitions in the Official Secrets Act along with the Criminal Code provisions on treason, extortion, bribery, and secret commissions. Apart possibly from the secret funding of Canadian voluntary activity, the impugned tactics are already unlawful or could be made so with minor amendments. With the one exception noted, the rationale for the existing law appears to cover the behaviour in question. This far at least, therefore, no genuine security interests would be compromised by confining the intrusive surveillance of citizens and residents to situations involving serious security-related law-breaking.

On the issue of the secret foreign funding of Canadian voluntary activity, we believe it cannot justify the intrusive surveillance of our citizens and residents. This is not to belittle the harm that might be done to our political processes by those who

appear to be genuinely indigenous participants while they are surreptitiously taking money (and perhaps even directions) from elsewhere. But, unless these people are breaking the law, we believe that they can and should be dealt with through the medium of democratic debate. Those of our citizens who slavishly parrot the many contortions of Soviet policy, for example, should be openly condemned by their political adversaries, not secretly spied on by government agencies. We believe that the democratic processes in this country deserve a higher level of confidence than this from our elected representatives.

Emergency Warrants

We are not persuaded by the SIRC proposal which would permit the by-passing of judicial warrants in emergency circumstances. Apparently, the current warrant-granting procedure involves a sixteen-stage process. In the event of a genuine emergency, there might be an argument for eliminating or reducing some of these stages. Indeed, there might even be a more expeditious exchange with the judge. In this regard, it is wise to remember how the Criminal Code has provided for telewarrants in exceptional circumstances. In any event, there is no excuse for the complete elimination of judicial scrutiny.

Security Evidence in the Courtroom

It is hard to appreciate what improvement would accrue to the administration of justice by the adoption of the SIRC proposal to exclude "the defendant and counsel as well as the public" from

criminal trials when security matters are raised. Such a procedure might be reasonably acceptable when the matters at issue involve resident status or classified employment. But our society could not as readily countenance the exclusion of the accused and their counsel when the matters at issue could involve incarceration and liberty. If there is security information that cannot be disclosed to the accused or the public, the judge should be required to consider how necessary such information is to the right of the accused to make full answer and defence. To whatever extent the judicial finding is that such information is necessary, there should be a dismissal of the charges against the accused.

NOTES AND SOURCES

1. "Security Chief resigns his post under pressure", Globe and Mail, September 12, 1987, p.A1.

2. "Unions resent infiltration by CSIS informers", Ottawa Citizen, October 3, 1987, p.B4; "CSIS not spying on unions, watchdog committee says", Globe and Mail, March 30, 1986, p.A4; and Security Intelligence Review Committee, Section 54 Report to the Solicitor General of Canada on CSIS' Use of Its Investigative Powers with Respect to the Labour Movement, March 25, 1988.

3. SIRC, Annual Report, 1986-87 (Ottawa: Supply and Services, 1987), pp.37,39.

4. SIRC, Annual Report, 1987-1988 (Ottawa: Supply and Services, 1988), p.1.

5. Affidavits of Margaret Third-Tsushima, Executive Director, St. Barnabas Refugee Society, May 10, 1989 and William Zander, President, British Columbia Provincial Council of Carpenters, May 10, 1989, respectively. The Corporation of the Canadian Civil Liberties Association v. The Attorney-General of Canada, RE 1193/89 (S.C.O.).

6. "CSIS probed Labrador Innu among other native groups", Globe and Mail, June 1, 1989, pp.A1,2; "Innu protesters spied on by Ottawa", Toronto Star, May 31, 1989, p.A13; "CSIS chief defends Innu probe: Soviet interference feared", Winnipeg Free Press, June 16, 1989, p.17.

7. SIRC, Annual Report, 1987-1988, p.31.

8. SIRC, Annual Report, 1988-1989 (Ottawa: Supply and Services, 1989), p.33.

9. The definition of "threats to the security of Canada" does not include lawful advocacy, protest or dissent unless carried on in conjunction with any of the activities specifically referred to. Canadian Security Intelligence Service Act, RSC 1985, c. C-23, s.2.

10. CSIS Act, s21(3) requires judicial warrants for surreptitious entry, mail opening, invasion of confidential records, and electronic bugging.

11. As an example of this preventive philosophy, consider the following remarks: "...The primary objective of an efficient intelligence service must be to prevent any insurgency or terrorism developing beyond the incipient stage. Hence a high quality intelligence service is required long before the insurgency surfaces." Paul Wilkinson, Terrorism and the Liberal State (Toronto: Macmillan of Canada, 1977), p.135; quoted by Canada, Commission of Inquiry Concerning Certain Activities of the RCMP (the "McDonald Commission"), Freedom and Security Under the Law,

Second Report, Vol. 1, p.436.

12. Quotation from GAO Audit of the FBI is found in U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Final Report, Book II: Intelligence Activities and the Rights of Americans, p.19, fn.108.

13. The GAO audit can be found in the Report to the House Committee on the Judiciary by the Comptroller General of the United States, FBI Domestic Intelligence Operations -- Their Purpose and Scope: Issues that Need to be Resolved (Washington, D.C.: GAO, February 24, 1976) pp.138-47.

14. "Additional Views of Senator Philip A. Hart", U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Final Report, Book II, p.359.

15. Testimony of Joseph Califano before the U.S. Senate Intelligence Committee cited in U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Final Report, Book II, p.19.

16. Omnibus Crime Control and Safe Streets Act, Title III, 18 U.S.C. 2516 (1968).

17. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. 1801.

18. Ibid., 101(b)(2)B. See also John T. Elliff, The Reform of FBI Intelligence Operations, pp.155-56.

19. In our 1984 brief on Bill C-9, for example, we argued that, in order to justify a surreptitious search, the security-related breach of the law should be directed by a foreign power (see submissions to House of Commons Committee on Justice and Legal Affairs re: Bill C-9 National Security from Canadian Civil Liberties Assocation, Ottawa, April 5, 1984). For purposes of this submission, however, our recommendations are confined to the introduction of a minimum standard for all intrusive surveillance. Any attempt to draw distinctions among the various surveillance techniques can be deferred until that goal is achieved.

20. Christine M. Marwick, "The Government Informer: A Threat to Political Freedom", First Principles, Vol.2, No.7 (March 1977), p.4.

21. Ibid., p.3.

22. Hoffa v. U.S. (1966), 385 U.S. 293, p.302.

23. Professor Ira S. Shapiro, "The Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and

the Fourth Amendment", (1977) 15 Harvard Journal on Legislation 119, p.173.

24. Senate of Canada, Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, Delicate Balance: A Security Intelligence Service in a Democratic Society (Ottawa: Supply and Services, 1983), p.22 .

25. Ibid., p.19.

26. SIRC, Section 54 Report to the Solicitor General of Canada on CSIS' Use of its Investigative Powers with Respect to the Labour Movement, March 25, 1988, p.14.

27. Clarence Kelly quoted by John T. Elliff in The Reform of FBI Intelligence Operations (Princeton, N.J.: Princeton University Press, 1979),p.77.

28. U.S. Senate, Report of the Select Committee on Intelligence, The FBI and CISPES, pp.1,12.

29. "RCMP security team may be rival of CSIS", Globe and Mail, July 4, 1989, pp.A1,2.

30. American Civil Liberties Union Submission on the National Intelligence Reorganization and Reform Act (s.2525) presented to the U.S. Senate Committee on Intelligence, July 18,1978, p.37.

31. McDonald Commission, Transcripts, Vol. 65, (July 18, 1978), pp.10593 ff. (regarding Exhibit D-26), and "Faked note to keep terrorists out of PQ...", Globe and Mail, July 19, 1978, p.9.

32. McDonald Commission, Transcripts, Vol. 65, (July 18, 1978 pp. 10619 and 10594-10595, respectively, (regarding Exhibit D-26).

33. McDonald Commission, Transcripts, Vol.65 (July 18,1978), p.107

34. Cabinet directive, March 27, 1975. See McDonald Commission, Freedom and Security Under the Law, Second Report, Vol. 1, p.75.

35. See McDonald Commission, Transcripts, Vol.27 (March 6, 1978), p.4394 (Exhibit D-1).

36. Kenneth Swan, "Whistle-Blowing and National Security", National Security: Surveillance and Accountability in a Democratic Society, eds. Peter Hanks and John D.McCamus (Cowansville, Que.:Les Editions Yvon Blais Inc., 1989), p.171.

37. McDonald Commission, Freedom and Security Under the Law, Second Report, Vol.1, pp.414-415,432-433.

SUMMARY OF RECOMMENDATIONS

Recommendation No. 1

Citizens and permanent residents should not be targeted for electronic bugging, mail opening, surreptitious entry, invasion of confidential records, or the deployment of covert informants unless, at the very least, there are reasonable grounds to believe that the matter under investigation involves a serious security-related breach of the law such as sabotage, espionage, serious violence, extortion, or bribery impairing the operations of government.

While some of these intrusive techniques should require even more exacting standards, none should be allowed on the basis of anything less.

Recommendation No. 2

The governing statute should contain provisions specifying:
a) the officials who must approve the deployment of covert informants and
b) guidelines for regulating the behaviour of such informants during undercover operations.

Recommendation No. 3

The Act should be restructured so as to require more demanding tests in order to authorize
a) more intrusive over less intrusive techniques of information gathering and
b) the surveillance of citizens and permanent residents over the surveillance of visitors.

Recommendation No. 4

The agency primarily charged with the collection of security intelligence should also have law enforcement duties with respect to the same matters.

Recommendation No. 5

There should be specific criteria governing the retention 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. 6

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

Recommendation No. 7

As regards SIRC, the following changes should be made:
a) the term of office should be substantially extended and made non-renewable
b) there should be access to everything relevant in the possession of CSIS and the government, including confidences of the Queen's Privy Council
c) whistle-blowers should be able to complain directly to SIRC and they should be granted immunity from identification and, if necessary, from discipline.
d) SIRC's jurisdiction should extend to every governmental operation involved in security intelligence activity.

Recommendation No. 8

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

Recommendation No. 9

There should be automatic reviews of the statute by Parliament every five years.