SUBMISSIONS TO - House of Commons Committee
on
Justice and Legal Affairs

RE - Bill C-9
National Security

FROM - Canadian Civil Liberties Association

DELEGATION - A. Alan Borovoy
(General Counsel)
Kenneth Swan
(Vice-President)

OTTAWA - April 5, 1984

Contents

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-9. 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 today, we do not, indeed we cannot, object to the performance of security and intelligence functions on behalf of the Canadian people and their institutions. 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 <u>statutory</u> 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-9 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.

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 our appearance before the Committee was arranged on relatively short notice, it will be appreciated that this brief is less than comprehensive. To whatever extent the Committee might wish additional comments, we would hope to provide them either at the hearing or at a later stage of the deliberations.

The Breadth of Surveillance

Standards For Intrusive Surveillance

Despite improvements over its predecessor, Bill C-9 would endow the new security and intelligence agency with 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 RCMP security service mandate, Bill C-9 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 Canadian citizens who, without any foreign direction whatever, took up a collection for the State of Israel in the wake of the Lebanese war? Or, suppose such citizens got similarly involved with the rebels in El Salvador or even Afghanistan?

By virtue of a later sub section, the Bill would make such intrusive surveillance available for "activities...intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada". When ultimate intentions become the operative threshhold, there is a great danger that speculation rather than evidence would be at a premium. What indeed would constitute acceptable evidence of an ultimate intention? Can the word "ultimately" deal with any point between now and the end of time? The more speculative the exercise becomes, the greater the risk of intruding on completely lawful behaviour.

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". "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.

Despite the government's attempts to assure us, Bill C-9 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, and "detrimental" interests.

Moreover, there are real doubts whether these dangers would be sufficiently diminished by the special exemption for "lawful advocacy, protest or dissent". It is not at all clear that such activities as fund raising or commercial negotiations would be embraced by these saving words. The problem is that there is a wide variety of lawful activities which may well not be described as advocacy, protest, or dissent.

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. As attractive as this approach might initially 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 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 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".[1] 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.[2] 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".[3] 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.[4]

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.[5] 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.[6]

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-9. 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 intrusive surveillance should not be permitted 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.[7]

Recommendation No. 1

Citizens and permanent residents should not be targeted for intrusive surveillance such as electronic bugging, mail opening, surreptitious entry, or invasion of confidential records without, at the very least, reasonable grounds to believe that there is a serious security related breach of the law such as sabotage, espionage, or serious violence impairing the operations of government. While some of these intrusive techniques should require more, none should be allowed on the basis of anything less.

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.[8]

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 urge a false egalitarianism.[9] 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. Such an argument was made, for example, by the Senate Committee which made recommendations on the previous Bill. Despite its argument for treating everyone alike, it nevertheless proposed that citizens and permanent residents be exempted as targets for the intelligence gathering contemplated by section 16 of the current Bill.[10]

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. 2

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 Techniques of Intrusive Surveillance

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.[11] During the course of this surveillance, however, the American authorities overheard more than 40,000 people in more than a half a million conversations.[12] 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.[13]

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.[14] 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.[15] In the case of federal security bugs, it lasted as long as 244.71 days.[16]

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 <u>doubt</u> 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".[17]

Former U.S. Attorney General Ramsey Clark contended that, if all security bugs were turned off, the impact on security would be "absolutely zero".[18]

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".[19]

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.[20] It is fair to infer that a knowledgable 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".[21]

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-9.

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.[22] 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.[23] 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.[24] 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.[25] 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.[26] 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. 3

> The electronic bugging of citizens and permanent residents, for security purposes, should require reasonable grounds to believe there is a serious security- related breach of the law directed by a foreign power. Apart from such foreign controlled threats, bugging should be governed entirely by the provisions of the Criminal Code.

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 exists the minimum circumstances which we have recommended for all intrusive surveillance - reasonable grounds to believe a serious security-related breach of the law is involved. 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 believe that the serious security-related breach of the law is being directed by a foreign power. As we indicate later, 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 controlled threats, entries against domestic operations should more often be

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

Again, our views are sustained by the American experience. U.S. law does not permit surreptitious entry, for intelligence purposes, against an essentially domestic threat.[27] What is even more significant is the absence of any concerted attempt to enact such a power in that country.

Recommendation No. 4

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.

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".[28] 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 believe there is 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.

Recommendation No. 5

Apart possibly from serious security related breaches of the law directed by a foreign power, citizens and permanent residents should be immune from mail opening in the course of post.

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-9 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.[29] Again, we believe that such access should not be permitted against citizens and permanent residents without, at a minimum, reasonable grounds to believe there is 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 and Bill C-9 has adopted such immunity for census information. The Commission made a particularly persuasive case 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..."[30]

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. 6

There should be no investigative access to income tax information relating to citizens and permanent residents. Special access to all other such personal information in government data banks should require, at the very least, reasonable grounds to believe there exists 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.[31] 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.[32]

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-9 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".[33] 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-9 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. 7

The governing statute should contain provisions specifying:

(a) the circumstances under which informants and infiltrators may be deployed,

(b) the officials who must approve such deployment, and

(c) the guidelines regulating the behaviour of informants and infiltrators during such undercover operations.

The Follow-Up To Surveillance

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. Morecver, 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-9 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-9 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 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. 8

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, Bill C-9 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.[34] 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...deterring, 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-9 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 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 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 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. 9

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 appreciates the fact that Bill C-9 will require judicial warrants for the most intrusive surveillance techniques. While such a safeguard is necessary, it is not sufficient. It is not likely to compensate adequately for any defects in the statute itself. To whatever extent a set of circumstances were to fall within the statutory criteria, judges would be very reluctant to withhold the warrants that were requested of them. That's why it is so important for the statutory powers to be drafted much more narrowly than is currently the case.

Nevertheless it would be desirable, as an additional safeguard, to empower the judges to refuse warrants in any situations where they believed that the intelligence to be gained did not outweigh the privacy which would be lost. Even if this discretion would be used only rarely, it would be better to have it than not to have it. In this regard, we note that such a recommendation was made by the Pitfield Committee.[35] We are not persuaded by the Government's argument that this provision is not needed because of the new stipulation that Ministerial approval will be required for all warrant applications. It will be recalled that one of the purposes of judicial warrants in the first place was to act as a check on the current warrant granting powers of the Minister.

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 agency. 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.

Recommendation No. 10

The courts granting warrants for intrusive surveillance should be entitled to consider whether, in their view, the intelligence to be gained outweighs the privacy to be lost.

Recommendation No. 11

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. 12

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

Structure

One of the key sources of danger in Bill C-9 is that virtually all of the investigations it contemplates are designed to serve intelligence rather than law enforcement purposes. Since the goal of an intelligence investigation is to assess, understand, and predict, the temptation will be to discover almost everything there is to know about the targets including their most intimate habits and beliefs. It is not hard to appreciate the chill that such pervasive surveillance can create to both political liberty and personal privacy.

A law enforcement investigation, on the other hand, 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.

There may be an argument for a certain amount of intelligence-centred surveillance in the case of security threats which emanate from foreign powers. 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 security 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. While there is sometimes an intelligence component even in more conventional criminal investigations, the goal, sooner or later, is to prosecute. In any event, the regular criminal law appears to apply intrusive techniques such as wiretapping and electronic bugging for law enforcement rather than intelligence purposes.

Unfortunately Bill-9 nowhere makes this distinction. Homegrown revolutionaries are made subject to the same intelligence centred focus as KGB agents. While we have had qualms about the creation of an all civilian intelligence gathering agency, we believe that its dangerous potential could be somewhat diminished if it were strictly confined to the arena of foreign directed security threats. What is crucial is that this agency should have no jurisdiction over essentially domestic security threats. Those threats should remain the responsibility of normal police agencies. Indeed, there might even be an argument for leaving domestic security threats with the RCMP. The split would be sensible.

Domestic security threats are essentially criminal in nature. They should be handled, therefore, by a police force which is involved in law enforcement. It is significant that, when the FBI's violations of civil liberties became public in the mid-1970's, the United States adopted the kind of approach we are recommending here. 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 cases as much as possible "like all other criminal cases".[36] In short, the narrower focus of criminal investigations was less likely to intrude on lawful dissent.

As a counter-intelligence entity against foreign threats, the new agency might have a somewhat wider information gathering function. For the reasons indicated, such counter-intelligence investigations often do not culminate in criminal prosecutions.

The adoption of such a split between foreign and domestic threats would provide a helpful structure for adjusting the surveillance powers as well. Foreign security threats would be the province of the new agency armed with a limited set of intelligence gathering powers in an amended new Bill. Domestic security threats would be under the jurisdiction of the police, perhaps the RCMP, armed only with the law enforcement powers of the Criminal Code.

Once such a split occurred, it would be important to ensure that the review mechanisms were imposed not only on the new agency which would be working in the foreign area but also on whatever police forces would be handling domestic matters. This country simply could not tolerate a return to the kind of unsupervised encroachments which characterized so much of the past RCMP wrongdoing.

Recommendation No.13

The jurisdiction for handling security and intelligence functions should be split as follows:

- The new agency armed with a limited set of intelligence gathering powers in an amended new Bill should be strictly confined to counter-intelligence against foreign controlled security threats
- The RCMP or other appropriate police forces, armed only with the law enforcement powers of the Criminal Code, should deal with essentially domestic security threats
- The safeguards, controls, and external review mechanisms should apply to all of the agencies involved in security and intelligence work including the RCMP and any other designated police force

Summary of Recommendations

Recommendation No. 1

Citizens and permanent residents should not be targeted for intrusive surveillance such as electronic bugging, mail opening, surreptitious entry, or invasion of confidential records without, at the very least, reasonable grounds to believe that there is a serious security related breach of the law such as sabotage, espionage, or serious violence impairing the operations of government. While some of these intrusive techniques should require more, none should be allowed on the basis of anything less.

Recommendation No. 2

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. 3

The electronic bugging of citizens and permanent residents, for security purposes, should require reasonable grounds to believe there is a serious security-related breach of the law directed by a foreign power. Apart from such foreign controlled threats, bugging should be governed entirely by the provisions of the Criminal Code.

Recommendation No. 4

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.

Recommendation No. 5

Apart possibly from serious security-related breaches of the law directed by a foreign power, citizens and permanent residents should be immune from mail opening in the course of the post.

Recommendation No. 6

There should be no investigative access to income tax information relating to citizens and permanent residents. Special access to all other such personal information in government data banks should require, at the very least, reasonable grounds to believe there exists a serious security-related breach of the law.

Recommendation No. 7

The governing statute should contain provisions specifying:

(a) the circumstances under which informants and infiltrators may be deployed,
(b) the officials who must approve such deployment, and
(c) the guidelines regulating the behaviour of informants and infiltrators during such undercover operations.

Recommendation No. 8

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. 9

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. 10

The courts granting warrants for intrusive surveillance should be entitled to consider whether, in their view, the intelligence to be gained outweighs the privacy to be lost.

Recommendation No. 11

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. 12

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

Recommendation No. 13

The jurisdiction for handling security and intelligence functions should be split as follows:

- The new agency armed with a limited set of intelligence gathering powers in an amended new Bill should be strictly confined to counter-intelligence against foreign controlled security threats
- The RCMP or other appropriate police forces, armed only with the law enforcement powers of the Criminal Code, should deal with essentially domestic security threats
- The safeguards, controls, and external review mechanisms should apply to all of the agencies involved in security and intelligence work including the RCMP and any other designated police force.

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. 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.
6. Foreign Intelligence Surveillance Act, Title 50, 30 U.S.C. §1801.
7. 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.
8. 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.
9. Regrettably, even the McDonald Commission rejected this distinction between residents and visitors. See Commission of Inquiry Concer Royal Canadian Mounted Police, Freedom and Security Under the Law Second Report Volume 1 (Ottawa: Queen's Printers, 1981) at 580.
10. Canada Parliament 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: Queen's Printers, 1983) at 22.
11. 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.
12. Schwartz, Herman, "A Report on the Costs and Benefits of Electronic Surveillance-1972", ACLU Report, March, 1973.
13. 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.
14. 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.
15. Canada, Parliament, Report of Solicitor General, Annual Report as Required by Section 178.22 of the Criminal Code, 1978.
16. Canada, Parliament, Report of Solicitor General, Annual Report as Required by Section16(5) of the Official Secrets Act, 1978.
17. 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.
18. Supra, fn.14, p.39.
19. Elliff, John T., The Reform of FBI Intelligence Operations (Princeton, New Jersey: Princeton University Press, 1979), p.41.
20. Supra. fn.14, p.40.
21. Ibid, p.39

22. The Criminal Code, R.S.C. 1970, Chap.C-34, s.178.1.
23. Ibid. Bugging under the Criminal Code contemplates, of course, a law enforcement rather than an intelligence gathering purpose. See also Elliff, supra, fn.19,p.159.
24. Foreign Agents Registration Act, Title 22, 11 U.S.C. § 611.
25. Supra, fn.5.
26. Supra, fn.6.
27. Supra, fn.5, § 2516 and 2518.
28. Supra, fn.9, p.575.
29. 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".
30. Supra, fn.9, p.587.
31. First Principles, published by Project on National Security and Civil Liberties, March 1977, Vol.2, Number 7, p.4.
32. Ibid, p.3.
33. Hoffa v. U.S. (1966),p.302.
34. Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police. Proceedings, vol. 65, pp. 10593-10643.
35. Supra, fn. 10, p. 21.
36. Supra, fn. 19, p. 190.