Date: 20060713

Docket: CSIS-18-05
Citation: 2008 FC 300

Ottawa, Ontario, this 13th day of July 2006

PRESENT: THE HONOURABLE MR. JUSTICE SIMON NOËL

IN THE MATTER OF an application by [...] for warrants pursuant to Sections 12 and 21 of the Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23

AND IN THE MATTER OF [...]

REASONS FOR ORDER AND ORDER

I. Introduction and Issues

[1] Pursuant to a Section 21 application of the *Canadian Security Intelligence Service Act, R.S.,* 1985, C. 23 (CSIS Act), the Canadian Security Intelligence Service (CSIS) is asking the Court, for the first time since the enactment of the CSIS Act, to issue warrants that [...]. The Deputy Attorney General of Canada (DAGC) is representing the CSIS.

[2] In order to ensure that this proceeding covers all of its potential implications, the Chief Justice assigned himself and the undersigned as Case Management Judges pursuant to Rule 383 of the *Federal Court Rules,* SOR/98-106 (the Rules).

[3] One of the main issues that this application brings up is a question of law [...]. The CSIS accepted after a hearing that an *Amicus Curiae* would be appointed by the Court and such appointment was made in the person of the Hon. Ron G. Atkey, P.C., Q.C. The need for an *Amicus Curiae* became evident since the CSIS could not objectively fully represent to the Court all the different points of views that the question of law brings up. It was clearly in the interest of justice that an *Amicus Curiae* should be appointed by the Court to deal with the opposite point of view presented by the CSIS to support the Application for warrants [...].

[4] A preliminary issue that was brought up by the undersigned was whether or not the question of law identified in the precedent paragraph could be dealt with separately from the warrants application, in a public hearing, or whether such question must be heard *in camera.* To put it differently, can this question of law be debated in a public hearing without prejudicing national security concerns considering the materials as filed before the Court? The mandate of the *Amicus Curiae* was enlarged to include the presentation of submissions on this preliminary issue.

[5] The *Amicus Curiae* argued that it would be feasible but the CSIS is objecting.

[6] Since the Court has brought up this preliminary issue as part of its case management duties pursuant to Rules 3, 4, 385 of the Rules, Reasons for Order and Order will be issued.

[7] At the core of the present matter is the interpretation of section 27 of the CSIS Act. It reads

as follows:

27. An application under section 21, 22 or 23 to a judge for a warrant or the renewal of a warrant shall be heard in private in accordance with regulations made under section 28.	27. Une demande de mandat ou de renouvellement de mandat faite à un juge en vertu de l'article 21, 22 ou 23 est entendue à huis clos en conformité avec les règlements d'application de l'article 28.

II. Submissions

A. *The DAGC*

[8] In short, the DAGC argues that a proper reading of Section 27 of the CSIS Act requires that warrant applications be heard in private and that no disclosure of the existence, details or outcome of the application can be made.

[9] The DAGC submits that the words Ain private@ inserted in Section 27 of the CSIS Act are not qualified in any manner nor are they limited in time and that where a statute provides for an *in camera* hearing, neither the Court on its own volition, nor the parties on consent, can by-pass the mandatory requirements of such an *in camera* hearing (see *Ruby v. Canada (Solicitor General)* [2002] 4 S.C.R. 3, at para. 58).

[10] In support of its argument that Section 27 cannot be extended to express something other than Ain private@, the DAGC draws the attention of the Court to Sections 48 and 52 of the CSIS Act. Section 48 provides that investigations of complaints conducted by the *Security Intelligence Review Committee* (SIRC) shall be conducted Ain private@. Section 52 of the same act provides for the issuance of reports to the Director, the Minister and the complainant, which include

recommendations. The DAGC also draws a parallel with Subsections 78d) and 78h) of the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 (IRPA). These provisions explicitly state that hearings are to be held Ain private@ but that a summary of the information or the evidence must be provided to the foreign national or permanent resident. Again, the DAGC submits that neither Section 27 of the CSIS Act nor any other sections included in part II does provide for the release of any sensitive information. In essence, the DAGC argues that if Parliament intended hearings to be held in public under section 27 of the CSIS Act, it would have stated so explicitly in the provision.

[11] It is also the contention of the DAGC that warrant applications issued pursuant to the *Criminal Code, R.S.C. 1985, c.* C-46 are conducted Ain private@ and that access to such applications and the ensuing orders, if granted, are not available until the warrants have been executed (see *Toronto Star Newspaper Ltd. v. Ontario*, [2005] 2 S.C.R. 188, at paras. 19 and 20 and *Vancouver Sun (Re)*, [2004] 2 S.C.R. 332 at paras. 33 to 38, 60 and 72). In the DAGC's view, there are no reasons to depart from the wording of Section 27 and from the above Supreme Court decision, subject to the particulars of a warrant application under the CSIS Act.

[12] The DAGC is also concerned with the consequences on CSIS' methods of investigation if the question of law was addressed and debated in public. Section 21 applications involve threats to the security of Canada and refer to methodologies utilized for obtaining information in a covert fashion. The present application makes no exception and does refer in detail to the methodologies to be used. In the past, the Federal Court has always protected such sensitive

information in accordance with long established jurisprudence (see *Henri v. Canada (Security Intelligence Review Committee), 140 N.R. 315,* [1992) F.C.J. No. 100). It is the opinion of the DAGC that the methodologies included in the present application are innovative approaches to the collection of information, and that it must be protected by the Court.

[13] Finally, it is submitted that the Court is seized with a warrant application pursuant to Section 21 of the CSIS Act, not a Motion for a Declaratory Judgment. The DAGC argues that a Motion for Declaratory Judgment would not be appropriate to address the question of law, and that to proceed with the said warrant application as if it were a Motion for Declaratory Judgment would be to do indirectly that which cannot be done directly.

[14] The DAGC notes that this Court in the past issued Reasons for Judgment (see files 84-01, 84-04, Tab 8 and 9 of DAGC's Submissions), which were helpful to establish guidelines. It is submitted that the same can be done with the present warrants application.

B. *The Amicus Curiae*

[15] It is admitted by the *Amicus Curiae* that some information must not become public and must
remain confidential such as: the target of the proposed warrant, the means of interception (the methodologies), the places where the warrant would be executed, etc. However, the *Amicus Curiae* argues that the jurisdictional issue should and could be debated in public.

[16] In order to protect the confidential information, the Amicus Curiae submits that the Court could rely on the CSIS Alegend@ entitled ACSIS National Security Claims@ (NSC) which establishes
the standard within the Government of Canada for determining what constitutes information that if
it were disclosed to the public would be Ainjurious to International Relations, National Defence or
National Security@. Information that is subject to NSC is defined as follows (see Written Submission of Ronald G. Atkey as *Amicus Curiae*, at para. 7)

> 1) Identify or tend to identify Service interest in individuals, groups or issues, including the existence or absence of past or present files or investigations, the intensity of investigations, or the degree or lack of success of investigations.
> 2) Identify or tend to identify human sources of information for the Service or content of information provided by a human source.
> 3) Identify or tend to identify investigative techniques and methods of operation utilized by the Service.
> 4) Identify or tend to identify Service employees or internal procedures and administrative methodologies of the Service, such as names and file numbers etc.
> 5) Identify or tend to identify relationships that the Service maintains with other police and security and intelligence agencies in Canada and elsewhere and would disclose information received in confidence from such sources.
> 6) Reveal or tend to reveal information concerning the telecommunications system utilized by the Service.
> 7) Jeopardize or tend to jeopardize essential international relations [emphasis in original].

By using such definition, the information contained in the application could be reviewed and such information could be excluded.

[17] After having noted that Section 27 of the CSIS Act refers to Regulations made under Section 28 and that such Regulations are non-existent, it is submitted by the *Amicus Curiae* that

the code for Judicial Control found in sections 21-28 is incomplete and that Section 27 must be tempered by rights and remedies prescribed by the *Federal Courts Act* (the Federal Courts Act) and the Rules.

[18] The Amicus *Curiae* presented two remedies provided for in the Federal Courts Act under which it would be possible to protect NSC information while at the same time hearing jurisdictional issues in public. It is specifically suggested that a Motion for Declaratory Judgment, pursuant to Sections 17 or 18 of the Federal Courts Act, would be appropriate avenues. In his submissions, the *Amicus Curiae* then explained how such procedures would be conducted, who would bring the action, which decision would be reviewed and what issues would be addressed. For the purposes of the present interim decision, it is not necessary to discuss in detail such matters. What is important to keep in mind is that the *Amicus Curiae* considers that there are proper avenues to consider in order to establish a public forum to address the issue of whether or not the CSIS Act gives the jurisdiction to the Federal Court to grant warrants [...] without divulging information that would prejudice International Relations, National Defense or National Security.

[19] Furthermore, in its argument, the *Amicus Curiae* informs that Section 27 of the CSIS Act is subject to the application of Section 2b) of the *Canadian Charter of Rights and Freedoms* (The Charter) and that there is a principle of open access to the Courts which has to be respected in order to foster confidence and ensure accountability (see *Vancouver Sun (Re)*, above, at paragraphs

24-26).

[20] In sum, it is the opinion of the *Amicus Curiae* that the issue of the interpretation of the CSIS Act should and could be dealt with publicly. In the *Amicus Curiae's* opinion, the Federal Court Act and the Rules provide for appropriate remedies, and the ACSIS National Security Claims@ categories would be useful for the Court to exclude, on a piece-by-piece basis, any information that could be injurious to International Relations, National Defense or National Security.

[21] In a subsidiary argument, the *Amicus Curiae* submits that at least the submissions of Counsel for both parties should be made public provided that such submissions do not include any National Security Claims information, the whole pursuant to Rule 4 (AMatters not provided for@) and Rule 109(3) (ADirections@ or AIntervention@).

III. Analysis

[22] Below I will first address the scheme of judicial control under Part II of the CSIS Act. Then I will turn to the interpretation of Section 27 and to the specifics of the present matter.

A. The Nature of a Warrant Application and the Judicial Control Regime under the CSIS Act

(1) History and Aims of the Judicial Control Regime under the CSIS Act

[23] Prior to the enactment of the CSIS Act, warrants were issued by the Solicitor General under the authority of Section 16 of the *Official Secrets Act, R.S.C. 1970,* c. O-3). Section 16 was added by an amendment to the Act in 1973.

[24] The idea that there should be judicial involvement in the warrant issuance procedures goes back to the early 1980's when the Commission of Inquiry concerning certain activities of the Royal Canadian Mounted Police (The Commission) published its report (see Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Second Report - Vol. *1 : Freedom and Security under the Law,* Ottawa, August 1981, pp. 592 to 594, paras. 179, 180, 181):

> 179. Our recommendations would make the security intelligence agency's use of four extraordinary powers conditional on obtaining a warrant from a Federal Court Judge. These four powers are the interception of communications by electronic surveillance, searches of private premises or property in circumstances in which a search warrant for criminal investigation would not be available, the examination of mail, and access to personal information other than `biographical information' held by the federal government. We refer to these powers as `extraordinary' because they involve acts which would be violations of law if carried out by ordinary citizens, and because, unlike special police powers, they may be exercised in circumstances where there is no evidence that a particular crime has been committed or is about to be committed. Two other techniques, which are not extraordinary in this sense, namely surveillance of private premises by hidden optical devices or cameras and the use of dial digit recorders, should also be subject to this system of control by judicial warrants.
>
> 180. Under our recommendations for controlling the level of investigation, the security intelligence agency could not initiate a request for a warrant to use any of these techniques to gather intelligence about a specific individual or group until a >full= investigation of that individual or group has been approved. It will be recalled that a decision to carry out a full investigation must be approved by the Solicitor General on a proposal which is supported by the Director General and has been carefully reviewed by a Committee which includes senior officers of the security agency as well as a lawyer from the Department of Justice and a senior official of the Solicitor General's Department. At the time the Solicitor

> General's approval of a full investigation is sought, the security agency might request his approval of an application to a judge for a warrant for a particular technique. It might conceivably at that time request his approval for applications for warrants for more than one technique, but in this case it would be extremely important for the security agency and the Solicitor General to give careful consideration to the necessity of using each technique. Every effort should be made to use only that method which is best calculated to enable the agency to complete an investigation with a minimum intrusion of privacy. We do not think that the various techniques requiring a judicial warrant can be scaled in terms of their inherent intrusiveness. Indeed, in some circumstances, the use of an undercover informant, which does not require a judicial warrant, may be regarded as a more intrusive and less effective means of obtaining information than one of the techniques which does.
>
> 181. In considering an application for a warrant to use two or more methods, the Federal Court Judge would have to consider the strength of the case which is made for the necessity of using each technique. He should also be informed when considering any application whether warrants have been issued for the use of other techniques in relation to the same subject of investigation and if they have what results they have produced. It is essential that the judge be in a position to consider whether, given what has been obtained or what can reasonably be expected to be obtained from other techniques, and given the statutory direction to minimize intrusions on privacy, the necessity of using a particular technique has been demonstrated [my emphasis].

The Commission felt that the involvement of the Federal Court in warrant procedures was necessary in order to ensure that the legal criteria established in the legislation were duly respected (see Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Second Report - Vol. 2: *Freedom and Security under the Law*, Ottawa, August 1981, p. 882, para. 5):

> Par. 5. [. .. J Because of the secret nature of these techniques and the absence of any provision requiring notification of persons subject to them, we felt that judicial authorization is the best way to ensure that the requirements of the law are met in each case [My emphasis].

[25] In 1983, a special committee of the Senate (The Senate Committee) examined the subject matter of Bill C-157 (the predecessor to Bill C-9, *An Act to establish the Canadian Security Intelligence Service, to enact An Act Respecting enforcement in relation to certain security and related offenses and to amend certain Acts in consequence thereof or in relation thereto,* 2d Sess., 32d Parliament, 1984 - which became the CSIS Act in 1984 - see *Canadian*

Security Intelligence Service Act, S.C. 1984, c. 21) and agreed with the Commission that warrants to be granted would give CSIS significant powers and that the Federal Court was the proper forum to have the warrant process reviewed and decided (see Canada, Senate of Canada, Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, A *Delicate Balance:* A *Security Intelligence Service in a Democratic Society,* November 1983, pp. 20 to 23, paras. 56 to 67).

[26] There are similarities between the objectives of a warrant application and the ones associated with a warrant application presented pursuant to the Criminal Code. Having said that, it is important to emphasize that their respective aims are totally different. The Senate Committee did

make that distinction when reviewing Bill C-157 (see Canada, Senate of Canada, Report of the Special Committee of the Senate on the Canadian Security Intelligence Service, above, paras. 13, 14, 15):

> 13. Once it is accepted that a distinct security intelligence capacity is required, cognizance must be taken of the fundamental differences between a system established for enforcement of the law, and a system established for the protection of security. There are similarities between such systems, and a distinct area of overlap in which the interests of a police force in certain crimes against the state, or against particular individuals, are identical to the interests of a security intelligence agency.
>
> 14. <u>But the differences are considerable.</u> Law enforcement is essentially reactive. While there is an element of information-gathering and prevention in law enforcement, on the whole it takes place after the commission of a distinct criminal offence. The protection of security relies less on reaction to events; it seeks advance warning of security threats, and is not necessarily concerned with breaches of the law. Considerable publicity accompanies and is an essential part of the enforcement of the law. Security intelligence work requires secrecy. Law enforcement is Aresult-oriented@, emphasizing apprehension and adjudication, and the players in the system - police, prosecutors, defense counsel, and the judiciary - operate with a

> high degree of autonomy. Security intelligence is, in contrast, Ainformation-oriented@. Participants have a much less clearly defined role, and direction and control within a hierarchical structure are vital. Finally, law enforcement is a virtually Aclosed@ system with finite limits - commission, detection, apprehension, adjudication. Security intelligence operations are much more open-ended. The emphasis is on investigation, analysis, and the formulation of intelligence.
>
> 15. The differences between law enforcement and the protection of security have profound implications for several aspects of a security intelligence regime. They can have effect on many questions of policy, such as how much power or freedom of action a person employed in a security agency should have; or obversely, how much protection a person who is the object of investigation can have in light of the differences between operational means and investigative ends. An investigation related to security can have severe consequences on a person's life. Thus the question of control and accountability becomes important, because there is no impartial adjudication by a third party of the appropriateness of an investigation. Since it is so open-ended and confidential in nature, security intelligence work requires a close and thorough system of control, direction and review, in which political responsibility plays a large part. Such close direction is incompatible with our traditional notions of law enforcement [my emphasis].

[27] In *Henrie v. Canada (Security Intelligence Review Committee), [1989]* 2 F.C. 229, at paras. 26-28, Justice Addy of the Federal Court recognized that the distinction of these two types of investigation had to be taken in consideration when assessing national security issues:

> &26 In considering whether the release of any particular information might prove injurious to national security and in estimating the possible extent of any such injury, one must bear in mind that the fundamental purpose of and indeed the raison d=être of a national security intelligence investigation is quite different and distinct from one pertaining to criminal law enforcement where there generally exists a completed offence providing a framework within the perimeters of which investigations must take place and can readily be confined. Their purpose is the obtaining of legally admissible evidence for criminal prosecutions. Security investigations on the other hand are carried out in order to gather information and intelligence and are generally directed towards predicting future events by identifying patterns in both past and present events.
>
> &27 There are few limits upon the kinds of security information, often obtained on a long-term basis, which may prove useful in identifying a threat. The latter might relate to any field of our national activities and it might be an immediate one or deliberately planned for some time in the relatively distant future. An item of information, which by itself might appear to be rather innocuous, will often, when considered with other information, prove extremely useful and even vital in identifying a threat. The very nature and source of the information more often than not renders it completely inadmissible as evidence in any court of law. Some of the information comes from exchanges of intelligence information between friendly countries of the western world and the [page242] source or method by which it is obtained is seldom revealed by the informing country.
>
> &28 Criminal investigations are generally carried out on a comparatively short-term basis while security investigations are carried on systematically over a period of years, as long as there is a

> reasonable suspicion of the existence of activities which would constitute a threat to the security of the nation [my emphasis).

[28] Warrants granted under the CSIS Act are extraordinary, intrusive, related to open-ended investigations, information-oriented with an emphasis on investigation, analysis and the formulation of intelligence. The persons of interest in such procedures can be related to countries of interest for Canada for the role they play as representatives, or they can be persons of interest because of their activities in relation to threats to the security of Canada as defined in Section 2 of the CSIS Act. As a consequence, there is a wide spectrum of potential targets. Because of the nature, invasiveness and sensitivity of the activities of CSIS, its modes of operations must be subject to a complete, closed system of control by the judiciary.

[29] In short, the AJudicial Control@ regime adopted in 1984 (Sections 21 to 28 - Part II of the CSIS Act) is aimed at both ensuring the lawfulness of the operations of the CSIS and the secrecy of the information that is disclosed to the Court in seeking and obtaining warrants. Below I explain these provisions of the CSIS Act.

(2) The Regime of Judicial Control under the CSIS Act

[30] The Director of CSIS or an employee designated for this purpose first presents, with the approval of the Minister of Public Safety and Emergency Preparedness, an application for the issuance of the warrant under subsection 21(1) of the CSIS Act

21. (1) Where the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate a threat to the security of Canada or to perform its duties and functions under section 16, the Director or employee may, after having obtained the approval of the Minister, make an application in accordance with subsection (2) to a judge for a warrant under this section.	21. (1) Le directeur ou un employé désigné à cette fin par le ministre peut, après avoir obtenu l'approbation du ministre, demander à un juge de décerner un mandat en conformité avec le présent article s'il a des motifs raisonnables de croire que le mandat est nécessaire pour permettre au Service de faire enquête sur des menaces envers la sécurité du Canada ou d'exercer les fonctions qui lui sont conférées en vertu de l'article 16.

[31] As per section paragraph 21(2)(a), the CSIS is required to explain, in a written application, its reasons for believing that the warrant is necessary to investigate threats to the security of Canada (Sections 2 and 12 of the CSIS Act) or to collect information concerning foreign states and persons (Section 16 of the CSIS Act). An affidavit must be filed in support of the application, as per Subsection 21(2). The affidavit must include the following:

- the facts relied on to justify the belief, on reasonable ground, that the issuance of warrants is required;
- the facts that other investigative techniques were not successful or would not be successful, that there is some urgency justifying not using conventional techniques and that without such warrants valuable information will be missed;
- the types of information being sought and the ones to be obtained by entering premises, removing information or otherwise;
- the identity of the persons or the groups of persons to be targeted by the warrant;
- a description of the places when the warrants would be executed where possible;
- the period of time of the existence of the warrants (60 days for investigations

related to paragraph (d) of the definition of the expression Athreat to the security of Canada@ in section 2 [activities led to the overthrow or destruction of Canada's system of government]) but no more than a year in all other cases;

- details about any previous applications related to the same individuals or groups.

[32] As per Subsection 21(4) and Section 23, warrants must specify the following:

- the types of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained;
- the identity of the person, if known, whose communication is to be intercepted or possesses the information, record, document or thing to be obtained;
- the identity of the person or classes of persons targeted by the warrant;

- the place(s) (with description if possible) to be accessed and searched and the possibility of removing any thing installed pursuant to a warrant;
- the duration of the warrant;
- any other terms and conditions that the judge may consider.

[33] Renewal of warrants is possible under Section 22 of the CSIS Act. The effect of the warrant is to give the necessary authority to whom it may concern to act in accordance with the said warrants, notwithstanding another law (see Sections 25, 26, 27 of the CSIS Act).

[34] Section 27 provides that applications for warrant Ashall be heard in private@ (Ahuis clos@

in

French). APrivate@ is defined as Aconfidential; secret@ in Brian A. Garner, *Black=s Law Dictionary*, 8th ed. (St-Paul: Thomson West, 2004), *s.v.* Aprivate@ In Hubert Reid, *Dictionnaire de droit québécois et canadien*, (Montréal, Wilson & Lafleur, 1994), *s.v.* Ahuis clos@, the expression Ahuis clos@ is described as being Aune exception au principe de la publicité des débats, qui consiste à interdire au public l=accès à la salle d=audience@. Again, the main aims of the privacy of applications for a warrant are to preserve the secrecy of sensitive information in general and to ensure the execution of warrant. The interested person(s) (targets) must not be present or aware of the warrant application; otherwise, its purpose would become academic. The public should not have access to the information because it is related to national security and because of the effectiveness of the CSIS depends on the secrecy of its methods and operations. Finally, third party information is often transmitted under the caveat that it would not be released. If warrants were debated in public, sensitive information would likely be released advertently or inadvertently. It would prevent the CSIS from being informed about threats to Canada=s security, would render useless the investigation, would be dangerous to human sources involved and could endanger Canada=s relationship with allied countries.

[35] In sum, designated judges' role pursuant to Part II of the CSIS Act is to exercise a judicial scrutiny on the lawfulness, necessity and reasonableness of the techniques of investigations of CSIS, keeping in mind that the privacy requirement of warrant applications is justified given the national security concerns at stake.

B. Substantive Considerations

(1) <u>National Security and Fundamental Rights</u>

[36] Warrant applications for national security purposes and intelligence gathering are topics that our Courts have not specifically dealt with. In deciding whether it is possible or not to deal in public with jurisdictional issues in relation to such applications, the Court has to consider both fundamental rights and national security concerns.

[37] In *Toronto Star Newspaper Ltd. v. Ontario*, [2005] 2 S.C.R 188, at paras. 1 to 3, Justice Fish made the following statement:

> & 1 In any constitutional climate, the administration of justice thrives on exposure to light -- and withers under a cloud of secrecy.
> & 2 That lesson of history is enshrined in the *Canadian Charter of Rights and Freedoms*. Section 2(b) of the *Charter* guarantees, in more comprehensive terms, freedom of communication and freedom of expression. These fundamental and closely related freedoms both depend for their vitality on public access to information of public interest. What goes on in the courts ought therefore to be, and manifestly is, of central concern to Canadians.
> & 3 The freedoms I have mentioned, though fundamental, are by no means absolute. [...]

[38] The present matter clearly brings up that basic freedoms protected by the *Canadian Charter of Rights and Freedoms* sometime have to be assessed in light of other values. Decisions made in a vacuum can sometime give way to detrimental situations even though they were made at first sight to protect our basic freedoms.

[39] Access to our Courts is fundamental to our democratic system. It allows public scrutiny of the judicial process, as well as media access to information of public interest. In that sense, freedom of expression is inextricably linked to the open courts principle. Transparency in the administration of justice fosters trust in the judicial system. It also protects the integrity of the judicial system in making sure that the rule of law prevails and helps to maintain the independence and impartiality of the Courts (see *Vancouver Sun (Re),* above, at paras. 23 to 26, by Chief Justice McLachlin for the majority). To deny public access to the Courts must be strongly justified in accordance with the situation at play and the valued principles at stake.

[40] National security has always been a subject of concern to our Courts when dealing with our basic fundamental rights. Under certain circumstances, it is necessary to balance national security with fundamental rights. This was emphasized in *Application under s. 83.23 of the Criminal Code (Re),* [2004] 2 S.C.R. 248. At paras. 5 to 7, Justices Iacobucci and Arbour wrote:

> & 5 The challenge for democracies in the battle against terrorism is not whether to respond, but rather how to do so. This is because Canadians value the importance of human life and liberty, and the protection of society through respect for the rule of law. Indeed, a democracy cannot exist without the rule of law . So, while Cicero long ago wrote *"inter arma silent leges"* (the laws are silent in battle) (Pro *Milone 14),* we, like others, must strongly disagree [...].
>
> & 6 Although terrorism necessarily changes the context in which the rule of law must operate, it does not call for the abdication of law. Yet, at the same time, while respect for the rule of law must be maintained in the response to terrorism, the Constitution is not a suicide pact, to paraphrase Jackson J.: *Terminiello v. Chicago, 337 U.S. 1 (1949),* at p. *37* (in dissent).
>
> &(7 Consequently, the challenge for a democratic state=s answer to terrorism calls for a balancing of what is required for an effective response to terrorism in a way that appropriately recognizes the fundamental values of the rule of law. In a democracy, not every response is available to meet the challenge of terrorism. At first blush, this may appear to be a disadvantage, but in reality, it is not. A response to terrorism within the rule of law preserves and enhances the cherished liberties that are essential to democracy. As eloquently put by President Aharon Barak of the Israeli Supreme Court [my emphasis):

> This is the fate of democracy, as not all means are acceptable to it, and not all methods employed by its enemies are open to it. Sometimes, a democracy must fight with one hand tied behind its back. Nonetheless, it has the upper hand. Preserving the rule of law and recognition of individual liberties constitute an important component of its understanding of security. At the end of the day, they strengthen its spirit and strength and allow it to overcome its difficulties.
>
> (H.C. 5100/94, *Public Committee Against Torture in Israel v. Israel,* 53(4) P.D. 817, at p. 845, cited in Barak, *supra*, at p. 148.)

[41] In *Henrie v. Canada (Security Intelligence Review Committee),* above, at para. 18, Justice Addy expressed a concern in balancing the principle of public access to the courts with the competing interest of the State in protecting national security:

> & 18 [...] Public interest in the administration of justice requires complete openness of the judicial process. That principle must be jealousy guarded and rigorously applied, especially where evidence which appears to be relevant to a judicial determination is at stake. That cardinal rule not only safeguards the rights of litigants generally but, more importantly, it is fundamental to the public interest in the preservation of our free and democratic society. There are, however, very limited and well-defined occasions where that principle of complete openness must play a secondary role and where, with regard to the admission of evidence, the public interest in not disclosing the evidence may outweigh the public interest in disclosure. This frequently occurs where national security is involved for the simple reason that the very existence of our free and democratic society as well as the continued protection of the rights of litigants ultimately depend on the security and continued existence of our nation and of its institutions and laws.

This reasoning was adopted by the Federal Court of Appeal in *Moumdjian v. Canada (Security Intelligence Review Committee), [* 1997] F.C.J. No. 1574, at para. 6.

[42] In my view, it is necessary to keep in mind this necessary balance between national security and fundamental rights to interpret Section 27 of the CSIS.

(2) Interpretation of Section 27 of the CSIS Act

(a) The *Warrant Application Itself*

[43] In the present matter, I have no doubt that the wording of Section 27 of the CSIS Act is very important. This imperative wording indicates the clear intention of Parliament that the hearing of the application for warrants A[...] be heard in private [...]@. Furthermore, the fact that the Governor in Council has not made Regulations in accordance with Section 28 of the CSIS Act, in relation to the forms of warrants, establishing procedures and security requirements for hearings does not in any way change the intent of the legislator.

[44] I agree, as emphasized by the DAGC, that it is not possible for a judge to allow a public hearing on the warrant application itself. The analogy proposed by the DAGC with the Supreme Court case *Ruby v. Canada (Solicitor General)*, above, is, in my view, correct. In this case, Justice Arbour, on behalf of the Court, commented on provisions of the *Privacy Act, R.S.C.*, c. P-21 that provides for a mandatory *in camera* and ex *parte* proceedings when an individual questions the decision of refusing access to personal exemption on grounds of national security or the maintenance of foreign confidence. Subsection 51(2) x) and 51(3) of the *Privacy Act* read as follows:

51. (2) An application referred to in subsection (1) or an appeal brought in respect of such application shall	51. (2) Les recours visés au paragraphe (1) font, en premier ressort ou en appel, l'objet d'une audition à huis clos; celle-ci a lieu dans la région de la capitale nationale définie à l'annexe de la Loi sur la capitale nationale si le responsable de l'institution fédérale concernée le demande.
(a) be heard in camera; and	
(b) on the request of the head of the government institution concerned, be heard and determined in the National Capital Region described in the schedule to the National Capital Act.	
[...]	[...]

(3) During the hearing of an application referred to in subsection (1) or an appeal brought in respect of such application, the head of the government institution concerned shall, on the request of the head of the institution, be given the opportunity to make representations ex parte.	(3) Le responsable de l'institution fédérale concernée a, au cours des auditions en première instance ou en appel et sur demande, le droit de présenter des arguments en l'absence d'une autre partie.

The wording is different from the one included in Section 27 of the CSIS Act but it basically expresses the same restrictions insofar as presence of the interested persons and access to the public are concerned.

[45] Justice Arbour mentioned, at paras. 57-58 that it is not possible for the judge to depart from the wording of these provisions and to allow a public hearing on the warrant application, except on constitutional issues:

> & 57 In our case, counsel for the Solicitor General informed the Court during oral argument that the hearing in this case before MacKay J. with respect to the merits of the exemptions claimed, was heard in camera. On the other hand, the hearings before Simpson J. on the constitutional questions were conducted in public. Counsel for the Solicitor General further represented to the Court that the Department of Justice has interpreted s. 51 narrowly, limiting the *in camera* requirement only to those portions of a hearing that concern the merits of the exemptions claimed under *s. 19(1) (a)* or (b) or s. 21 but allowing the Crown to consent to Acollateral@ issues (i.e., constitutional or procedural issues) being heard in open court.
>
> & 58 Aside from the constitutional issue, the Solicitor General's interpretation of s. 51(2) (a) is not one that the statute can reasonably bear. Section 51(2)(a) mandates that the hearing of an application under s. 41 and an appeal therefrom relating to personal information that a government institution has refused to disclose by reason of s. 19(1)(a) or (b) or s. 21 be heard *in camera*. Contrary to the apparent practice referred to by the Solicitor General, the statute does not limit the *in camera* requirement to only those parts of a hearing that involve the merits of an exemption. It is not open to the parties, even on consent, to bypass the mandatory *in* camera requirements of s. 51. Nor is open to a judge to conduct a hearing in open court in direct contradiction to the requirements of the statute regardless of the proposal put forth by the parties. Unless the mandatory requirement is found to be unconstitutional and the section is Aread down@ as a constitutional [page35] remedy, it cannot otherwise be interpreted to bypass its mandatory nature [my emphasis].

Therefore, it is my view that I have no discretion to authorize a public hearing on the warrant application itself under Section 27 of the CSIS Act. This, however, should be qualified with

respect to Acollateral@ issues.

(b) A*Collateral*@ Issues

[46] In my view, issues that are Acollateral@ to a warrant application, such as jurisdictional issues,

could be heard in open courts in some circumstances. It is to be noted that there are no regulations made under Section 28 of the CSIS Act to provide guidance to the Court in deciding what should remain confidential.

[47] In this context, I believe that each case turns on its facts keeping in mind the clear wording of Section 27 of the CSIS Act and the necessary balance between national security and fundamental rights. In some circumstances, to debate a jurisdictional, procedural or constitutional question in public can be injurious to national security or prevent the proper execution of a warrant. It is also possible to imagine cases where the public hearing would be allowed on some of the issues of law, while others would remain confidential. Below I assess the specific of the present matter to determine whether it would be possible to allow a public hearing on the jurisdictional issue.

[48] The following portion *of* the *Henrie v. Canada,* above, is also instructive as to the nature of information the disclosure of which would be injurious to national security. At para. 29, Justice Addy wrote, at para. 29:

> & 29 When considering the issue of the relative merits of the public interest in non-disclosure as opposed to the public interest in disclosure, it is evident that the considerations and circumstances to be taken into account which might militate against the proper control or suppression of threats to national security are considerably more numerous and much more complex than the considerations which involve a national interest other than those mentioned in section 36.2 of the Canada Evidence Act. In criminal matters, the proper functioning of the investigative efficiency of the administration of justice only requires that, wherever the situation demands it, the identity of certain human sources of information remain concealed. By contrast, in security matters, there is a requirement to not only protect the identity of human sources of information but to recognize that the following types of information might require to be protected with due regard of course to the administration of justice and more particularly to the openness of its proceedings: information pertaining to the identity of targets of the surveillance whether they be individuals or groups, the technical means and sources of surveillance, the methods of operation of the service, the identity of certain members of the service itself, the telecommunications and cypher systems and, at times, the very fact that a surveillance is being or is not being carried out. This means for instance that evidence, which of itself might not be of any particular use in actually identifying the threat, might nevertheless require to be protected if the mere divulging of the fact that CSIS is in possession of it would alert the targeted organization to the fact that it is in fact subject to electronic surveillance or to a wiretap or to a leak from some human source within the organization.

[49] At para. 30, he went on to say the following about releasing information (which in itself is neutral) and on the understanding that an informed person could have:

> & 30 It is of some importance to realize than an Ainformed reader@, that is, a person who is both [page243] knowledgeable regarding security matters and is a member of or associated with a group which constitutes a threat or a potential threat to the security of Canada, will be quite familiar with the minute details of its organization and of the ramifications of its operations regarding which our security service might well be relatively uninformed. As a result, such an informed reader may at times by fitting a piece of apparently innocuous information into the general picture which he has before him, be in a position to arrive at some damaging deductions regarding the investigation of a particular threat or of many other threats to national security. He might, for instance, be in a position to determine one or more of the following: (1) the duration, scope intensity and degree of success or of lack of success of an investigation; (2) the investigative techniques of the service; (3) the typographic and teleprinter systems employed by CSIS; (4) internal security procedures; (5) the nature and content of other classified documents; (6) the identities of service personnel or of other persons involved in an investigation [my emphasis].

This portion of Justice Addy's decision was cited numerous times by this Court: it is often described as the Amosaic effect@ (see *Zundel (Re),* 2005 FC 195, at para. 109). In numerous cases, the Federal Court cited these two paragraphs a reference for deciding whether releasing information would be detrimental to national security (see, for example, *Alemu v. Canada*

(Minister of Citizenship and Immigration), 2004 FC 997, at para. 14; *Harkat (Re),* 2003 FCT 285,; at para. 20).

(3) Assessment of the Facts before the Court

[50] In the matter at hand, the *Amicus Curiae* submits that it is possible to address, in public, the issue of whether or not the CSIS Act grants the Federal Court jurisdiction to issue warrants which [...]. The question before the Court is therefore whether it is possible to address this issue without breaching the intent of Parliament.

[51] The facts and the documents before the Court led me to the conclusion that it is not possible to debate in public of the jurisdictional issue.

[52] First, the fact of raising the question in public, in itself, would reveal [...], it would be injurious to national security and to the operations of the CSIS to reveal it.

[53] [...] CSIS operates abroad through the work of intelligence officers. Indeed, Mr. Jack Hooper, Deputy Director (Operations) of the CSIS stated before a Senate Committee that Canada is active abroad (see Canada, Senate of Canada, Standing Committee on National Security and Defence, May 29, 2006):

> [...]
>
> **Senator Campbell**: [...] Is the CSIS overseas role focused entirely on the collection of intelligence about threats to the security of Canada? How are Canada's foreign intelligence requirements being

addressed?

Mr. Hooper: The law actually does not permit us to collect foreign intelligence outside Canada - Aforeign@ intelligence being intelligence around the intentions and capabilities of foreign states and persons. Typically, when people talk about foreign intelligence, at least under our legal model, they are talking about political, economic and military intelligence. In response to your first question, senator, everything we do abroad is directed at collecting security intelligence.

In terms of how we do that, we are moving from one model to another. The service has historically, and the RCMP security service before it, posted what we call security liaison officers in many countries. The primary function of these officers was to conduct liaison with other trusted intelligence organizations and law enforcement agencies.

Afghanistan is a circumstance that has reoriented our thinking about what we need to be doing abroad. It taught us the lesson that much of the information on domestic threats has to be obtained outside the country.

We do that through a variety of means. We do it through foreign collection officers, visiting case officers and the use of assets whom we task and direct to collect intelligence abroad. There are a number of means, not the least of which is our interaction with allied intelligence services in an international arena.

Senator Campbell: How many people would you have working overseas gathering information? These would be your liaison officers, I take it.

Mr. Hooper: We have something less than 50 intelligence officers abroad.

Senator Campbell: Since the number of terrorist groups and individuals has stayed relatively constant, have we expanded our capabilities since 1998? While I recognize it has remained static, I think the threat has continued to increase. Have you been able to increase your overseas staff since 1998?

Mr. Hooper: Not to the extent that we would like. We received funding in two envelopes over the last two years to augment our foreign collection program, and a lot of that money was earmarked for sending people abroad.

Over the past number of years we have borrowed from domestic collection programs and the people doing that work to send them abroad to do foreign collection. We have invested the money that government accorded us at the front end, in various kinds of infrastructure support, because we can spend that money immediately. It takes a little longer to recruit and train a person who can then go abroad or who can backfill for someone already operating internationally.
[...]

It is public that CSIS is present overseas [...].

[54] Another consideration led me to the conclusion that it is not possible to address the jurisdictional issue in public: the issues of law and of fact are intertwined. In some circumstances,

questions of facts and questions of law are so inextricably linked that it is not possible to address the issue of law in a vacuum. This was noted by the Supreme Court of Canada, in the context of terrorism, in *Application under s. 83.23 of the Criminal Code (Re),* above, at paras. 30-31:

> & 30 To begin with, although specific provisions of the Act are directly before us, there are other sections that may be implicated on which we do not wish to pronounce absent a factual foundation. As well, we intend to decide only what is necessary to resolve the specific dispute in issue. We hope otherwise, but there will likely be other cases to arise for further elucidation, and we prefer to await that development.
>
> & 31 In addition context in the law is of vital importance and that is certainly the case with respect to terrorism What we say in these reasons is influenced by the adjudicative facts we have before us Although constitutional opinion on legislative facts is a different exercise, again, we wish to emphasize how important it is to examine the particular factual setting of each case prior to determining the legally required result [my emphasis].

[55] As the DAGC submits, addressing the question of law in public could have the effect of informing of methodologies utilized for obtaining information in a covert fashion. An application for warrants has been filed which has to be dealt with pursuant to the CSIS Act with all its specifications. Another avenue to deal with the question of law was not chosen by CSIS. This Court has to deal with the warrant application as it is filed. Questions of fact and the questions of law are inextricably linked in the application: it would be impossible, in this context, to debate in public of the issues of law without unveiling sensitive information, which would be damaging to national security.

[56] A public debate on the issue of law would be likely to reveal CSIS= methodologies. The question of law in itself does not contain such information. However, the application as it is filed cannot be separated in questions of facts and questions of law.

In the present circumstances, I do not think that the question of law can be fully dealt with in a vacuum. The question of law would raise several underlying questions, such as:

- How will that be done?
- How will warrant be executed [...]?
- Who will execute the warrant?
- Who will be involved?
- What types of warrants are being sought?
- Who is targeted?

For obvious reasons, answers to these questions cannot be given. The DAGC and the *Amicus Curiae* would have to argue on these questions. Their submissions could divulge to the public some methodologies of the CSIS and certain activities [...]. This is likely to restrain counsel for the DAGC to inform the designated judge about information that is relevant to the questions of law to be decided. In contrast, if the debate is conducted *in camera*, the judge will have all the relevant information before him and the debate is more likely to be comprehensive.

C. Conclusion

[57] Having noted that the question of law does trigger the automatic consideration of the facts related to the application for warrants and having identified some of the possible

consequences of discussing the question of law, I have to come to the conclusion that the jurisdictional issue as presented can not be dealt with in public. If a motion for declaratory judgment on the jurisdictional issue only (without factual evidence) would have been presented, then it would have been possible to seriously consider hearing it publicly. Such was not the decision taken by the CSIS.

[58] Finally, I understand that the wording used in Section 27 of the CSIS Act can be interpreted as being limitative to hearings to be held in private. In contrast, one can argue that Section 27 wording, although very clear as to the privacy of the hearing on the warrant application itself, mentions neither that the decision, nor the documents filed with the Court, are also Aprivate@. I leave for the Trial Judge to decide this issue, after having given the parties the opportunity to address it.

Having said that, I will be asking the Counsel by directive, whether or not the present decision or some parts of it can be made public.

[59] Pending further decision, the Reasons for Order and Order are to be kept *Ain private@.*

THEREFORE, THIS COURT ISSUES THE FOLLOWING ORDER:

- The Section 21 Application shall be heard Ain private@.

ASimon Noël@

_____

Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CSIS-18-05
STYLE OF CAUSE:	IN THE MATTER OF an application by [...] for warrants pursuant to Sections 12 and 21 of the Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23
PLACE OF HEARING:	Ottawa, Ontario
DATE OF HEARING:	June 30, 2005, December 20, 2005, January 11, 2006, March 10, 2006, March 31, 2006, May 10, 2006, May 12, 2006
REASONS FOR ORDER AND ORDER:	The Honourable Mr. Justice Simon Noël
DATED:	July 13, 2006

APPEARANCES:

Mr. John O'Halloran Mr. Robert F. Batt	For the Applicant
Mr. Ronald G. Atkey, P.C., Q.C.	Amicus Curiae

SOLICITORS OF RECORD:

Mr. John H. Sims, Q.C. Deputy Attorney General of Canada Ottawa, Ontario	For the Applicant