Federal Court  Cour fédérale

Date: 20131025

Docket: DES-7-08

Citation: 2013 FC 1096

Ottawa, Ontario, October 25, 2013

PRESENT: The Honourable Mr. Justice Blanchard

BETWEEN:

IN THE MATTER OF A CERTIFICATE SIGNED PURSUANT TO SUBSECTION 77(1) OF THE *IMMIGRATION AND REFUGEE PROTECTION ACT (IRPA);*

AND IN THE MATTER OF THE REFERRAL OF A CERTIFICATE TO THE FEDERAL COURT PURSUANT TO SUBSECTION 77(1) OF THE *IRPA;*

AND IN THE MATTER OF MOHAMED ZEKI MAHJOUB

REASONS FOR ORDER AND ORDER

[1] Mr. Mohamed Zeki Mahjoub is the named person in security certificate proceedings initiated pursuant to subsection 77(1) of the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 [*IRPA*]. In the course of these proceedings, the Ministers have adduced evidence in support of their case that was obtained or derived from several warrants issued under

section 21 of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 [*CSIS Act*]. These reasons dispose of a motion brought by Mr. Mahjoub to exclude this evidence.

Relief Sought

[2] In his "RE-MODIFIED NOTICE OF MOTION," Mr. Mahjoub sets out his request for relief as follows:

> a. An order quashing the warrants issued under sections 21, 22 or 23 of the *Canadian Security Intelligence Service Act* (or *CSIS Act*) ;
>
> b. An order excluding all evidence and information obtained from the warrants pursuant to subsections 24(1) and (2) of the Charter;
>
> c. An order excluding all evidence and information obtained illegally, and/or in violation of sections 7 and 8 of the Charter and in the course of procedures declared unconstitutional (*Charkaoui v. Canada*, [2007] 1 S.C.R. 350) pursuant to subsections 24(1) and/or (2) of the Charter and
>
> d. A declaration as to the violation of the applicant's rights as protected under sections 7 and 8 of the Charter;
>
> e. An order reserving the applicant his right to seek a permanent stay of proceedings pursuant to section 24(1) of the Charter for the Charter violations suffered;
>
> f. Any other remedy that the Court find [*sic*] just and appropriate;
>
> g. A declaration that the part of section 2 defining a "threat to the security of Canada" with sections 12 and 21 - 24 of the *CSIS Act* are unconstitutional and with [*sic*] no force or effect, as per section 52 of the *Constitution Act*, 1982, in that these sections unjustifiably violate sections 2, 7, 8 of the Charter;

Mr. Mahjoub seeks this relief pursuant to paragraph 399(1)(*a*) of the *Federal Courts Rules*, SOR/98-106 and section 18 of the *Federal Courts Act*, R.S.C. 1985, c. F-7.

Facts

[3] Prior to the issuance of the first security certificate in June 2000 under subsection 77(1) of the *IRPA* naming Mr. Mahjoub, the Canadian Security Intelligence Service (CSIS or the Service) applied to a designated judge of the Federal Court of Canada pursuant to section 21 of the *CSIS Act* for warrants allowing for the interception of some of Mr. Mahjoub's communications. One or more of these warrants was in operation after Mr. Mahjoub's arrest on June 26, 2000. Disclosure of the specifics of the warrants obtained by the Service during its investigation of Mr. Mahjoub would, in my opinion, be injurious to national security or the safety of persons. An overview of the warrants is therefore found in the "Facts" section of the Confidential Annex.

[4] When the Ministers signed the second security certificate on February 22, 2008, certifying that Mr. Mahjoub is inadmissible to Canada on the grounds of national security, the Security Intelligence Report (SIR) on which they relied contained information obtained as a result of the section 21 warrants. That information is contained at the following paragraphs in the SIR:

(a) Paragraph 6: *In July 1999, MAHJOUB's Canadian wife, Mona El-Fouli, was convinced that MAHJOUB would only stay married to her until such time as he received his citizenship papers.* This is an intercepted communication: see Revised Summaries of Conversations and Surveillance Reports, April 6, 2010, Tab 7.

(b) Paragraph 6: *In addition, on the day of MAHJOUB's arrest (June 26, 2000) El Fouli stated that she had decided to marry MAHJOUB because "all she knew that he was a 'mujahed' (holy fighter) and her marriage to MAHJOUB would bring her, and her son (Hani), closer to God".* This is an intercepted communication: see Revised Summaries of Conversations and Surveillance Reports, April 6, 2010, Tab 9.

(c) Paragraph 25: *MAHJOUB was a close associate of Mohamed Hafez Marzouk…* This is based upon telephone toll records, see paragraph (d) below.

(d) Paragraph 26: *After MAHJOUB's arrival in Canada, he contacted Marzouk by telephone. A telephone at MAHJOUB's residence was in regular contact with the cellular telephone of Marzouk from 1997 until Marzouk left Canada in May 1998*. This allegation is based upon telephone toll records, which show that there were 11 calls between a telephone at MAHJOUB's residence and the cellular telephone of Marzouk.

(e) Paragraph 31: *When an associate of MAHJOUB's inquired about MAHJOUB's news, MAHJOUB stated that he preferred to talk face to face, and reluctantly explained that he could not delve into the subject right then because of the presence of the "Moukhabarat" (i.e. secret services). In turn, this same associate asked whether MAHJOUB was referring to the civil or military "Moukhabarat" to which MAHJOUB replied "both"*. This is an intercepted communication: see Revised Summaries of Conversations and Surveillance Reports, April 6, 2010, Tab 8.

(f) Paragraph 32: *In July 2001, MAHJOUB, while in detention, got in touch with Mona El Fouli and inquired whether "she still had her telephone number on the old number", to which she replied in the affirmative. MAHJOUB commented that he should not be blamed if one of his ex-inmates got hold of El Fouli's new number because of that and advised her to cancel the forwarding service. El Fouli in turn stated that she would provide him with a possibly different telephone number where he could contact her. El Fouli preferred to provide him with the telephone number later*. This is an intercepted communication: see Revised Summaries of Conversations and Surveillance Reports, April 6, 2010, Tab 10.

(Sourced from a Communication from the Court dated September 23, 2010)

Items (a) and (b) have already been excluded from these proceedings following the Court's June 19, 2012 Order.

[5] On October 3, 2008, in the context of its review of the security certificate pursuant to subsection 77(1) of the *IRPA* (the reasonableness proceeding), this Court ordered the

disclosure of the section 21 warrants and supporting affidavits to the Special Advocates in accordance with the Ministers' disclosure obligations outlined in *Charkaoui v. Canada (Citizenship and Immigration)*, 2008 SCC 38 [*Charkaoui II*]. On December 15, 2008 and January 15, 2009, the materials were disclosed to the Special Advocates, and summaries of the disclosed material were eventually provided to Public Counsel on October 5, 2010.

[6] On August 3, 2010, Mr. Mahjoub submitted an "informal request" by letter to the Court seeking an Order requiring the Ministers "to communicate to Mr. Mahjoub all the warrants, affidavits, exhibits and transcripts in relation with the intercepts/searches/investigations mentioned in the Security Intelligence Report for the purpose of challenging said warrants." He filed a formal Notice of Motion for such disclosure on August 31, 2010.

[7] In a Direction, dated August 31, 2010, the Court explained that the legality of the section 21 warrants was not at issue in any of the motions previously brought by the Special Advocates. This fact was further confirmed at paragraphs 41, 45 and 55 of the Court's September 13, 2010 Communication. Mr. Mahjoub filed his Motion Record for his August 31, 2010 disclosure motion on September 20, 2010.

[8] On October 5, 2010, summaries of five warrants and five supporting affidavits were prepared collaboratively and ordered on consent to be disclosed to Mr. Mahjoub and his counsel pursuant to the Court's October 4, 2010 Reasons for Order.

[9] On October 25, 2010, Mr. Mahjoub brought his motion challenging the constitutional validity of the section 21 warrants, the admissibility of the evidence obtained pursuant to these warrants, and the constitutionality of sections 2, 6, 12, 17 and 21, 22, 23, and 24 of the *CSIS Act*. Mr. Mahjoub in a separate motion, of which the Attorneys general were notified, also challenges the constitutionality of these same sections of the *CSIS Act*. It is appropriate to deal with the latter challenge at this stage in the context of the within motion as the constitutionality of the *CSIS Act* has decisive bearing on the legality of the warrants.

Preliminary Issues

[10] The Ministers argue that the Court's August 31, 2010 Order (2010 FC 937) is dispositive of Mr. Mahjoub's motion to exclude the evidence obtained by the warrants authorized under section 21 of the *CSIS Act*. That Order implemented the Court's decision to exclude certain evidence pursuant to subsection 83(1.1) of the *IRPA* (2010 FC 787). The Ministers also argue that the within motion is duplicative of the Special Advocates' motion, the motion to exclude evidence pursuant to subsection 83(1.1), which resulted in the August 31, 2010 Reasons for Order and Order and is consequently abusive.

[11] The Ministers rely on the following paragraph of the August 31, 2010 Reasons for Order and Order:

> [66] I am of the view that the information in the supporting affidavit, not sourced from [redacted] interrogation, was sufficient to justify on reasonable grounds the belief that the warrant powers to intercept Mr. Mahjoub's private communications were required

> for the Service to investigate a threat to the security of Canada pursuant to the requirements of s.21 of the *CSIS Act*… Consequently, the information obtained and relied on by the Ministers from the intercepted communications obtained as a result of the Warrant [redacted] is admissible.

[12] The motion brought by the Special Advocates on behalf of Mr. Mahjoub and the resulting Reasons and Order concerned the narrow issue of inadmissibility of evidence by operation of subsection 83(1.1) of the *IRPA*. Mr. Mahjoub in this motion now challenges the validity of the warrants on the basis of the alleged unconstitutionality of the *CSIS Act*, the Service's alleged failure to provide full, fair and frank disclosure, and on the alleged non-compliance of the warrants with the *CSIS Act*. These issues were not before the Court at the time of the section 83(1.1) motion and were not considered in the June 9, 2010 Reasons for Order.

[13] The Ministers contend that the Special Advocates considered the issue and decided not to challenge the validity of the warrants. The Ministers appear to suggest that it is too late for Public Counsel to do so. The Ministers also contend that Mr. Mahjoub should not be allowed to re-litigate issues that have already been decided.

[14] The Ministers are correct that it is not open to Mr. Mahjoub to re-litigate issues that have already been decided by the Court. Mr. Mahjoub is estopped from bringing duplicative motions. See: *Toronto (City) v. CUPE, Local 79*, 2003 SCC 63 and *British Columbia (Workers' Compensation Board) v. Figliola*, 2011 SCC 52 at paragraph 24. However, while the Special Advocates must represent Mr. Mahjoub's interests *in camera*, they are not his counsel. Their decision to refrain from bringing a particular

motion should not therefore bind Mr. Mahjoub and his counsel. Put differently, Mr. Mahjoub should not be estopped from bringing a motion on an issue that the Special Advocates have said they will not raise.

Issues

[15] I will address the following issues on this motion:

1. Are certain provisions of the *CSIS Act* unconstitutional?
   (a) Are sections 2, 6 and 12 of the *CSIS Act* unconstitutional for vagueness or overbreadth?
   (b) Is section 17 of the *CSIS Act* unconstitutional because it authorizes CSIS to enter into intelligence-sharing arrangements with foreign agencies that have poor human rights records?
   (c) Are sections 21, 22, 23 and 24 of the *CSIS Act* unconstitutional for authorizing unreasonable search and seizure?

2. Can the lawfulness of the section 21 warrants be challenged, and if so, in what way?
   (a) Does the doctrine of collateral attack preclude challenge to the validity of the section 21 warrants in the context of determining the admissibility of evidence pursuant to section 24 of the *Charter of Rights and Freedoms*, Part I to the *Constitution Act, 1982*, c. 11 (U.K.), Schedule B [*Charter*] in a security certificate proceeding?

(b) Is the evidence obtained pursuant to the section 21 warrants inadmissible because *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9 [*Charkaoui I*] declared the previous *IRPA* regime, which was the law at the time the evidence was collected, unconstitutional?

(c) Does the non-disclosure of the confidential section 21 warrants and affidavits in support of the warrants to Mr. Mahjoub violate Mr. Mahjoub's right to full answer and defence?

(d) In the context of a challenge to section 21 warrants in a security certificate proceeding, can the Court consider the confidential affidavits, or must the Court restrict its consideration to the summary of the affidavits disclosed to Mr. Mahjoub?

3. Are the section 21 warrants themselves unlawful by reason of:

(a) The presence of information derived from torture in the supporting affidavits?

(b) CSIS's breach of the duty of full, fair and frank disclosure by presenting misleading affidavits to the designated judge that also omitted exculpatory information?

(c) The absence of any indication that the warrants complied with the requirements of the *CSIS Act*, namely subsection 21(1) and paragraphs 21(2)(*a*) to (*g*)?

(d) The warrants' authorization of solicitor-client interceptions, which constitutes unreasonable search and seizure?

4. Did CSIS engage in searches and seizures that were not authorized by the section 21 warrants and not otherwise authorized by law?

5. If evidence used in this proceeding was unlawfully obtained for any of the above reasons, should it nevertheless be admitted pursuant to subsection 24(2) of the *Charter*?

Analysis

[16] Mr. Mahjoub raised the issue of the constitutionality of the *CSIS Act* in the context of his general constitutional challenge to the proceeding. As stated above, I will deal with this issue at this juncture. In my view, it is more germane to the warrants motion than to the challenge to Division 9 of the *IRPA*. My conclusions here are intended to dispose of the issue and to inform my conclusions in the abuse of process and reasonableness decisions.

[17] The above noted issues will be considered in turn.

1. *Are certain provisions of the* CSIS Act *unconstitutional?*

   (a) *Are sections 2, 6 and 12 of the* CSIS Act *unconstitutional for vagueness or overbreadth?*

Section 2 and Section 12

[18] Mr. Mahjoub challenges the term "threats to the security of Canada" in sections 2 and 12 of the *CSIS Act*, alleging that they are vague and overbroad, infringing section 7 of the *Charter*. For ease of reference, I reproduce the impugned provisions below.

2. In this Act,	**2.** Les définitions qui suivent s'appliquent à la présente loi.
"threats to the security of Canada" *« menaces envers la sécurité du Canada »* "threats to the security of Canada" means	« menaces envers la sécurité du Canada » *"threats to the security of Canada"* « menaces envers la sécurité du Canada » Constituent des menaces envers la sécurité du Canada les activités suivantes :
(*a*) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,	*a*) l'espionnage ou le sabotage visant le Canada ou préjudiciables à ses intérêts, ainsi que les activités tendant à favoriser ce genre d'espionnage ou de sabotage;
(*b*) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,	*b*) les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque;
(*c*) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and	*c*) les activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique, religieux ou idéologique au Canada ou dans un État étranger;
(*d*) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally	*d*) les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat

established system of government in Canada,	ou ultime est sa destruction ou son renversement, par la violence.
but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*).	La présente définition ne vise toutefois pas les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord qui n'ont aucun lien avec les activités mentionnées aux alinéas *a*) à *d*).
12. The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.	**12.** Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard.
[Emphasis added]	[Je souligne]

[19] A similarly-worded provision, paragraph 53(1)(*b*) of the former *Immigration Act*, R.S.C. 1985, c. I-2, withstood constitutional scrutiny in *Suresh v. Canada (Minister of Citizenship and Immigration)*, 2002 SCC 1. At paragraph 2, the Supreme Court of Canada explained that "danger to the security of Canada" was under attack for vagueness. Examining the provision through the lens of *R. v. Nova Scotia Pharmaceutical Society*, [1992] 2 S.C.R. 606 [*Nova Scotia Pharmaceutical Society*], the Supreme Court concluded at paragraphs 83 and 92 that the phrase is not unconstitutionally vague

although it is difficult to define, "highly fact-based and political in a general sense" (at paragraph 85). The Court did not insist on direct proof of a specific threat to Canada to define this term, but it did require that there "be real and serious possibility of adverse effect to Canada" that is potentially serious (at paragraphs 88-89).

[20] Further, in *Nova Scotia Pharmaceutical Society*, the Supreme Court explained at page 643 that "a law will be found unconstitutionally vague if it so lacks in precision as not to give sufficient guidance for legal debate." At page 632, the Supreme Court stated that legislation must:

> (1) give citizens fair notice of the consequences of their conduct, and
>
> (2) limit law enforcement discretion.

[21] The legislation itself defines "threats to the security of Canada" in a detailed manner in paragraphs (*a*) to (*d*). These paragraphs clearly define those activities that may be considered a threat and specifically exclude lawful advocacy and dissent. I am of the view that the impugned provisions provide fair notice to the citizen and appropriately limit the Service's investigative discretion.

[22] Mr. Mahjoub cites the case of Ernst Zündel as an example of the definition's vagueness: a Holocaust-denier captured by this provision and by the inadmissibility provisions of the *IRPA*. However, Justice Blais (as he then was) at paragraph 6 of *Zündel (Re)*, 2005 FC 295, explained:

> It is important to note that Mr. Zündel's views on the Holocaust had been known for years, but were of no concern to the Canadian

> Security Intelligence Service (CSIS). They may well have been an irritant to many and may have been considered as vile and perverse, but they were not enough to label him as a security threat. Rather, the investigations only began when Mr. Zündel crossed the boundaries of free speech and pursuant to the Ministers' opinion, entered the realm of incitement to hatred and potential political violence in relation to the White Supremacist Movement.

The Court found that is was not because of Zündel's views on the Holocaust that he was considered a security threat, but rather because of the threat of political violence. In my view, *Zündel* falls well within the ambit of a restricted definition of "threats to the security of Canada." It is not an example of vagueness of the impugned language of the *CSIS Act*.

[23] In Mr. Mahjoub's case, the investigation of his potential membership in terrorist groups and activities linked with terrorism is also related to a threat of political violence. As such, it also comes within the ambit of a restricted definition of "threats to the security of Canada."

[24] The test for overbreadth is found in *R. v. Heywood*, [1994] 3 S.C.R. 761 at page 793 (and used in *R. v. Khawaja*, 2012 SCC 69 at paragraph 37). If legislation is overbroad, it is such that "in some applications the law is arbitrary or disproportionate" to the state interests it seeks to advance.

[25] The internal restrictions found in sections 2 and 12 of the *CSIS Act* define the Service's scope of discretion by specifically defining "threats to the security of Canada" and only permitting the Service to collect information "to the extent that it is strictly necessary". Further, the "threat" can only be investigated on reasonable grounds to

suspect standard. Based on the limitations and requirements imposed on the Service by the above cited provisions, I find that the sections at issue are neither arbitrary nor disproportionate to the state interests that they seek to advance. I conclude that the provisions are not overbroad.

[26] Mr. Mahjoub next appears to argue by implication that section 12 of the *CSIS Act* authorized unreasonable searches and seizures that engage his section 7 privacy rights, thereby violating his section 8 *Charter* rights.

[27] Mr. Mahjoub's main concern appears to be that the Service does not require "reasonable and probable grounds" to investigate an individual. He argues that the "reasonable grounds to suspect" standard in section 12 is too low and thereby results in an unreasonable search and seizure. He relies on *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145 [*Hunter*], the landmark decision of the Supreme Court of Canada interpreting section 8 of the *Charter*. In that case, the Supreme Court established that for a search to be reasonable, it requires reasonable and probable grounds that an offence is committed and that there is evidence to be found as a result of the search.

[28] Section 12 is about the collection of intelligence on activities that are suspected threats to the security of Canada. "Search" is defined as an investigative technique by the state that diminishes the reasonable expectation of privacy of a person (*Hunter* at pages 159-160; *R. v. Gomboc*, 2010 SCC 55 at paragraph 77), and "seizure" is defined as "taking of a thing from a person by a public authority without that person's consent" (*R.*

v. *Dyment*, [1988] 2 S.C.R. 417 at page 431, *R. v*. *Buhay*, 2003 SCC 30 at paragraph 33). There is typically no reasonable expectation of privacy if the individual does not keep the information in question private, for example in *R. v*. *Edwards*, [1996] 1 S.C.R. 128, the Court found that an individual did not have a reasonable expectation of privacy in his girlfriend's apartment. There is also no reasonable expectation of privacy in garbage (*R. v*. *Krist*, 100 C.C.C. (3d) 58 (BCCA)).

[29] According to *R. v*. *Collins*, [1987] 1 S.C.R. 265 at page 278, a search is reasonable without prior judicial authorization if it is authorized by a reasonable law and conducted in a reasonable manner. Since Mr. Mahjoub has raised no allegations that any searches conducted pursuant to section 12 of the *CSIS Act* were conducted in an unreasonable manner, I will address whether section 12 of the *CSIS Act* is a reasonable law.

[30] In *R. v*. *Kang-Brown*, 2008 SCC 18 [*Kang-Brown*] and *R. v A.M.*, 2008 SCC 1, the Supreme Court determined that the threshold for using a certain common law-authorized investigative technique, namely dogs trained in drug detection or "sniffer dogs", was "reasonable suspicion", a lower threshold than "reasonable and probable grounds" as described in *Hunter*. The recent companion cases *R. v*. *Chehil*, 2013 SCC 49 [*Chehil*] and *R. v*. *MacKenzie*, 2013 SCC 50 [*MacKenzie*] addressed another challenge to this standard and upheld the "reasonable suspicion" standard for deploying the sniffer dogs. Using sniffer dogs can be done without prior judicial authorization because "they are minimally intrusive, narrowly targeted, and can be highly accurate" (*Chehil* at

paragraph 1). As Justice Karakatsanis wrote in *Chehil* at paragraph 6, "[t]he reasonable suspicion standard requires that the entirety of the circumstances, inculpatory and exculpatory, be assessed to determine whether there are objective ascertainable grounds to suspect that an individual is involved in criminal behaviour." There must be a constellation of factors (or a single factor such as travelling under a false name) that is particularized enough to prevent indiscriminate or discriminatory searches (at paragraphs 30-31, 35). In addition, there must be a "nexus" between the factors and the criminal conduct, even if the factors are not themselves criminal conduct (at paragraph 37).

[31] The learned judge further commented in *Chehil* at pararaph 23 that "[b]oth the impact on privacy interests and the importance of the law enforcement objective play a role in determining the level of justification required for the state to intrude upon the privacy interest in question." She concluded at paragraph 24 that the appropriate justification for a search lies along a spectrum depending on these factors.

[32] The public interest in the Service investigating threats to the security of Canada is great. Nevertheless, section 12 of the *CSIS Act* does not, on its face, constrain the investigative techniques that may be used by the Service. In addition, unlike sniffer dog searches, under normal circumstances there is no judicial scrutiny for techniques employed pursuant to section 12, for the search is typically conducted unbeknownst to the target individual. It is therefore useful to examine the legislative constraints on section 12 and which techniques are actually employed by the Service pursuant to section

12 in order to determine whether the "reasonable suspicion" standard strikes the correct balance in these circumstances.

[33] While section 12 appears to be broad in scope, it is nonetheless constrained by the warrant requirements, namely sections 21 to 24 of the *CSIS Act*. Parliament intended these provisions to be used in circumstances where the investigation required interference with an individual's reasonable expectation of privacy. In such cases, the Service is required to obtain judicial authorization. Under the warrant process, the threshold is higher than that required for section 12 activities. To request a warrant an affiant on behalf of the Service must attest to "the facts relied on to justify the belief, 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…" (section 21(1) of the *CSIS Act*). Consequently, section 12 does not authorize intrusive searches and seizures of private information.

[34] In the "Amended Final Response to Questions Re: National Security Privilege Objections" prepared by the Service and dated March 5, 2012 (Exhibit R82), the Service disclosed a significant portion of its policies dealing with investigative techniques pursuant to section 12, as follows:

1. OPS-101 2006, Level 1 investigative techniques allowed include reporting of open information, querying federal/provincial/territorial/municipal records and databanks, querying records held by foreign police/security/intelligence organizations. Level 1 is

valid for 90 days and terminated immediately if the Service discovers that the activities of a target do not constitute a threat.

2. OPS-102 2006, Level 2, techniques allowed include level 1, use of physical surveillance, interview of the target or any other person who may have relevant information, and tasking of human sources. Level 2 is valid for 2 years.
3. OPS-103 2006, Level 3, techniques allowed include levels 1 and 2, use of physical surveillance, and application for or execution of warrant powers of Federal Court warrants. It is valid for 2 years.

It is also clear from the evidence that higher levels require higher authorization within the Service.

[35] I am satisfied, on a review of the techniques enumerated in the Service policies above, that they are minimally intrusive, if they engage a reasonable expectation of privacy at all. The "reasonable suspicion" standard must be satisfied in order to employ these techniques. Further, the policies contemplate obtaining Federal Court warrants, governed by sections 21 to 24, for more intrusive techniques. In my view, section 12 of the *CSIS Act*, as interpreted by the Service, requires the Service to have an objective, particularized basis for the use of any minimally intrusive investigative techniques and strikes the appropriate balance between the public interest in investigating threats to the security of Canada and the individual target's privacy rights.

[36] The Ministers argue that Parliament has legislated a lower standard than that required by *Hunter*, thereby allowing an intrusive search to be conducted on reasonable grounds to suspect standard, relying on *Kang-Brown* at paragraphs 3, 10, and 13. While I

accept that Parliament has the authority to legislate a lower standard for such searches and seizures, it is not apparent to me that Parliament has done so by enacting section 12 of the *CSIS Act*. Intrusive searches and seizures require a warrant pursuant to section 21.

[37] Disclosure of activities specifically undertaken by the Service in relation to Mr. Mahjoub under the authority of section 12 would, in my opinion, be injurious to national security or the safety of persons. The specifics of what was done can therefore be found in "Section A" of the Confidential Annex.

[38] The following paragraphs are a summary of my findings on this issue from the Confidential Annex.

[39] In my view, on the basis of the record, all of the techniques used pursuant to section 12 of the *CSIS Act* were minimally intrusive, and none of them were employed in a discriminatory or indiscriminate way.

[40] Further, Mr. Mahjoub and the Special Advocates have raised no specific facts which would indicate that specific techniques authorized by section 12 constitute unreasonable search and seizure. They have not argued that the Service did not have reasonable grounds to suspect that Mr. Mahjoub was connected to a threat to the security of Canada, nor have they argued that any particular technique failed to respect the balance between public and privacy interests. It was necessary for them to do so in order

for the Court to assess a particular technique according to the requirements set out in *Chehil* and *MacKenzie*.

[41] Mr. Mahjoub also challenges section 12 of the *CSIS Act* as it apparently permits Service personnel to obtain statements from him pertinent to his security certificate case without his knowledge, which he claims is an infringement of section 13 of the *Charter* against self-incrimination. Mr. Mahjoub, in his anaemic submissions on this issue, has failed to establish any ground upon which section 12 of the *CSIS Act* could be found to be unconstitutional on the basis of section 13 of the *Charter*. Section 12 is concerned with investigating threats to the security of Canada, not obtaining statements for an immigration proceeding. These allegations pertain to the conduct of the Service in collecting and using the information gathered under the authority of section 12, not to the constitutional validity of the provision itself.

[42] For the above reasons, I find that Mr. Mahjoub's constitutional challenge to section 12 of the *CSIS Act* is without merit.

Section 6

[43] Section 6 of the *CSIS Act* gives the Director of the Service, under the direction of the Minister, the control and management of the Service and all matters connected therewith. Mr. Mahjoub alleges that the provision enables several unconstitutional policies and guidelines.

[44] For ease of reference, I reproduce the impugned provision below:

6. (1) The Director, under the direction of the Minister, has the control and management of the Service and all matters connected therewith.	**6.** (1) Sous la direction du ministre, le directeur est chargé de la gestion du Service et de tout ce qui s'y rattache.
(2) In providing the direction referred to in subsection (1), the Minister may issue to the Director written directions with respect to the Service and a copy of any such direction shall, forthwith after it is issued, be given to the Review Committee.	(2) Dans l'exercice de son pouvoir de direction visé au paragraphe (1), le ministre peut donner par écrit au directeur des instructions concernant le Service; un exemplaire de celles-ci est transmis au comité de surveillance dès qu'elles sont données.
…	[…]
(4) The Director shall, in relation to every 12-month period or any lesser period that is specified by the Minister, submit to the Minister, at any times that the Minister specifies, reports with respect to the Service's operational activities during that period, and shall cause the Review Committee to be given a copy of each such report.	(4) Pour chaque période de douze mois d'activités opérationnelles du Service ou pour les périodes inférieures à douze mois et aux moments précisés par le ministre, le directeur présente à celui-ci des rapports sur ces activités; il en fait remettre un exemplaire au comité de surveillance.

[45] Even if it were established, as alleged, that executive action performed under an enabling statute is unconstitutional, this does not render the statute itself unconstitutional (*Commission des droits de la personne v. Attorney General of Canada*, [1982] 1 S.C.R. 215 at page 216). Mr. Mahjoub has failed to show how the provision at issue falls afoul of the *Charter* or his *Charter* rights. Further, while certain policies or executive action

enacted pursuant to the section might engage Mr. Mahjoub's individual rights, the provision itself does not.

[46] I have dealt with Mr. Mahjoub's challenges to individual policies and practices, insofar as they have been raised, in the *Abuse of Process Decision*.

(b) *Is section 17 of the* CSIS Act *unconstitutional because it authorizes CSIS to enter into intelligence-sharing arrangements with foreign agencies with poor human rights records?*

[47] Mr. Mahjoub alleges that section 17 of the *CSIS Act* is unconstitutional because it violates individuals' right to privacy pursuant to section 7 of the *Charter*. It enables intelligence-sharing arrangements with intelligence agencies having poor human rights records, and it therefore has the potential to enable sharing of personal information.

[48] For ease of reference, I reproduce the impugned provision below:

17. (1) For the purpose of performing its duties and functions under this Act, the Service may,	**17.** (1) Dans l'exercice des fonctions qui lui sont conférées en vertu de la présente loi, le Service peut :
(*a*) with the approval of the Minister, enter into an arrangement or otherwise cooperate with	*a*) avec l'approbation du ministre, conclure des ententes ou, d'une façon générale, coopérer avec :
(i) any department of the Government of Canada or the government of a province or any department thereof, or	(i) les ministères du gouvernement du Canada, le gouvernement d'une province ou l'un de ses ministères,
(ii) any police force in a province, with the approval of the Minister responsible for	(ii) un service de police en place dans une province, avec l'approbation du ministre

policing in the province; or	provincial chargé des questions de police;
(*b*) with the approval of the Minister after consultation by the Minister with the Minister of Foreign Affairs, enter into an arrangement or otherwise cooperate with the government of a foreign state or an institution thereof or an international organization of states or an institution thereof.	*b*) avec l'approbation du ministre, après consultation entre celui-ci et le ministre des Affaires étrangères, conclure des ententes ou, d'une façon générale, coopérer avec le gouvernement d'un État étranger ou l'une de ses institutions, ou une organisation internationale d'États ou l'une de ses institutions.
(2) Where a written arrangement is entered into pursuant to subsection (1) or subsection 13(2) or (3), a copy thereof shall be given forthwith to the Review Committee.	(2) Un exemplaire du texte des ententes écrites conclues en vertu du paragraphe (1) ou des paragraphes 13(2) ou (3) est transmis au comité de surveillance immédiatement après leur conclusion.

[49] Mr. Mahjoub's challenge is relevant to paragraph 17(1)(*b*) and not to the other provisions, so I shall examine that provision only.

[50] This provision authorizes the Service, with Ministerial approval, to enter into an arrangement or otherwise cooperate with foreign governments or agencies after consultation with the Minister of Foreign Affairs and International Trade. It is consequently assumed that in completing the arrangement, Department of Foreign Affairs and International Trade (DFAIT) input relating to country conditions was properly obtained and considered. The terms of that cooperation are then left to the Minister and

the Service to arrange. I accept that one of the purposes of arrangements made under this provision may be information-sharing.

[51] The provision governing the creation of the arrangements, paragraph 17(1)(*b*), is constrained by the requirement of consultation with the Minister of Foreign Affairs and International Trade, a minister with particular expertise in country conditions including human rights. This ensures that the Minister of Public Safety is informed about the country in question and has independent advice from outside of the Service and his or her department.

[52] Other legislative provisions further govern the information-sharing aspect of section 17 arrangements. Pursuant to subsection 8(2) of the *Privacy Act*, R.S.C. 1985, c. P-21 [*Privacy Act*], the Service may disclose personal information for the purpose of furthering the objectives of the *CSIS Act*. Paragraphs 8(2)(*f*) and (*m*), provide that:

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed	(2) Sous réserve d'autres lois fédérales, la communication des renseignements personnels qui relèvent d'une institution fédérale est autorisée dans les cas suivants :
…	[…]
(*f*) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the council of the Westbank First Nation, the council of a participating First Nation — as defined in subsection 2(1)	*f*) communication aux termes d'accords ou d'ententes conclus d'une part entre le gouvernement du Canada ou l'un de ses organismes et, d'autre part, le gouvernement d'une province ou d'un État étranger, une organisation internationale d'États ou de

of the First Nations Jurisdiction over Education in British Columbia Act —, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;	gouvernements, le conseil de la première nation de Westbank, le conseil de la première nation participante — au sens du paragraphe 2(1) de la Loi sur la compétence des premières nations en matière d'éducation en Colombie-Britannique — ou l'un de leurs organismes, en vue de l'application des lois ou pour la tenue d'enquêtes licites;
…	[…]
(*m*) for any purpose where, in the opinion of the head of the institution,	*m*) communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :
(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure	(i) des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée,
[Emphasis added]	[Je souligne]

[53] If the Service provides an individual's personal information to foreign agencies under section 17 arrangements for the purposes of investigating threats to the security of Canada, the Service's actions are also subject to paragraphs 8(2)(*f*) or (*m*).

[54] Paragraph 8(2)(*f*) of the *Privacy Act* has withstood constitutional scrutiny under sections 7 and 8 of the *Charter* in the extradition context, where personal information was shared with foreign law enforcement agencies. Paragraphs 13-14 of *United States of America v. Lucero-Echegoyen*, 2011 BCSC 1028 and paragraphs 28-34 of *United States*

of America v. Wakeling, 2011 BCSC 165 [*Wakeling*], examine the provision in light of a section 7 and section 8 challenge. The British Columbia Superior Court concludes that the provision is constitutional because it strikes the right balance between protecting the "residual privacy interests which are significantly diminished in this case" and "the important state interest in unimpeded and timely sharing of lawfully obtained information between law enforcement agencies to ensure the effective investigation of criminal activity with inter-jurisdictional dimensions" (*Wakeling* at paragraph 33).

[55] While normally disclosure of interceptions of private conversations is criminal, paragraph 193(2)(*e*) of the *Criminal Code*, R.S.C. 1985, c. C-46 [*Criminal Code*], allows disclosure made "to a person or authority with responsibility in a foreign state for the investigation or prosecution of offences and intended to be in the interests of the administration of justice in Canada or elsewhere…" Although Part II of the *Criminal Code*, which includes paragraph 193(2)(*e*) does not apply to the Service by reason of section 26 of the *CSIS Act*. The *CSIS Act* instead contains subsection 19(2), a provision analogous to paragraph 193(2)(*e*) of the *Criminal Code*. For ease of reference, I reproduce subsection 19(2) below:

19. (2) The Service may disclose information referred to in subsection (1) for the purposes of the performance of its duties and functions under this Act or the administration or enforcement of this Act or as required by any other law and may also disclose such information	**19.** 2) Le Service peut, en vue de l'exercice des fonctions qui lui sont conférées en vertu de la présente loi ou pour l'exécution ou le contrôle d'application de celle-ci, ou en conformité avec les exigences d'une autre règle de droit, communiquer les informations visées au paragraphe (1). Il peut aussi les communiquer aux autorités ou personnes

	suivantes :
(*a*) where the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada or a province, to a peace officer having jurisdiction to investigate the alleged contravention and to the Attorney General of Canada and the Attorney General of the province in which proceedings in respect of the alleged contravention may be taken;	*a*) lorsqu'elles peuvent servir dans le cadre d'une enquête ou de poursuites relatives à une infraction présumée à une loi fédérale ou provinciale, aux agents de la paix compétents pour mener l'enquête, au procureur général du Canada et au procureur général de la province où des poursuites peuvent être intentées à l'égard de cette infraction;
(*b*) where the information relates to the conduct of the international affairs of Canada, to the Minister of Foreign Affairs or a person designated by the Minister of Foreign Affairs for the purpose;	*b*) lorsqu'elles concernent la conduite des affaires internationales du Canada, au ministre des Affaires étrangères ou à la personne qu'il désigne à cette fin;
(*c*) where the information is relevant to the defence of Canada, to the Minister of National Defence or a person designated by the Minister of National Defence for the purpose; or	*c*) lorsqu'elles concernent la défense du Canada, au ministre de la Défense nationale ou à la personne qu'il désigne à cette fin;
(*d*) where, in the opinion of the Minister, disclosure of the information to any minister of the Crown or person in the federal public administration is essential in the public interest and that interest clearly outweighs any invasion of privacy that could result from the disclosure, to that minister or person.	*d*) lorsque, selon le ministre, leur communication à un ministre ou à une personne appartenant à l'administration publique fédérale est essentielle pour des raisons d'intérêt public et que celles-ci justifient nettement une éventuelle violation de la vie privée, à ce ministre ou à cette personne.

[56] Both section 193(2)(*e*) of the *Criminal Code* (the analogous provision to section 19(2) of the *CSIS Act*) and paragraph 8(2)(*f*) of the *Privacy Act*, survived a constitutional challenge in the context of RCMP wiretaps given to the United States authorities for the purposes of extradition. In *United States of America v. Wakeling*, 2012 BCCA 397, the appeal decision of 2011 BCSC 165 (leave to appeal to the Supreme Court granted) both paragraph 8(2)(*f*) of the *Privacy Act* and paragraph 193(2)(*e*) of the *Criminal Code* were raised, and the British Columbia Court of Appeal found the *Criminal Code* to be the determinative issue.

[57] At paragraph 34, the Court of Appeal held that "disclosure to other administration of justice officers, domestic and foreign, is an equally obvious and necessary exception [to the criminality of wiretap disclosure in the *Criminal Code*] without the necessity of further judicial authorization or further notice." While the Court of Appeal recognizes a reasonable expectation of privacy in judicially authorized interceptions of private communications (the disclosure of which normally would be criminal according to subsection 193(1) of the *Criminal Code*), it rejects the appellant's argument that Parliament should protect his conversations from being used in a criminal investigation "when and where required for that purpose" (at paragraph 39). The Court of Appeal further explains at paragraph 43 that:

> The information gathered by lawful electronic interception becomes law enforcement intelligence. In my opinion, it is no different than information obtained from a police informer or information contained in documents that lawfully come into the hands of the police. If disclosure is in the interests of the administration of justice, there is no need for prior judicial approval or for notice or for reporting. Such requirements would formalize and hamper the inter-jurisdictional investigation of crime

> and sometimes the prevention of crime. Control of the use of lawfully-gathered police intelligence by foreign authorities is not practical and would be presumptuous. What is practical and necessary for both crime detection and crime prevention is the ability of police officers to lawfully inform their counterparts in other jurisdictions about impending criminal activity, as occurred in the present case, or past criminal activity.

[58] In my view, the above reasoning finds application in this case. Specifically, it applies to disclosure of information over which Mr. Mahjoub has a reasonable expectation of privacy in conjunction with paragraph 8(2)(*f*) of the *Privacy Act*. Mr. Mahjoub argues that the sharing of intelligence obtained by warrant between the Service and other intelligence agencies, when done in order to further the Service's mandate to inform and advise the Government of Canada about threats to national security, re-engages his rights to privacy and constitutes an additional search or seizure. To accept this argument would formalize and hamper the inter-jurisdictional investigation of threats to the security of Canada. Further, disclosure of information to foreign agencies is reasonable if the public interest in disclosure outweighs the intrusion into the privacy of the individual.

[59] Section 17 of the *CSIS Act* must be understood in the context of these constraining statutory provisions. The overarching restriction on sharing personal information with foreign agencies, found in both the *CSIS Act* and the *Privacy Act*, is that the Minister and the Service must craft arrangements appropriately and determine on a case-by-case basis whether the public interest that will be served in sharing the information outweighs the violation of the individual's privacy.

[60] In this case, the balancing would be between the public interest in national security and the "residual" and "diminished" expectation of privacy Mr. Mahjoub has in the Service's intelligence concerning him. Further diminishing his expectation of privacy is the fact that Mr. Mahjoub was a foreign national applying for immigration status in Canada, and he therefore consented to security screening and the use of the personal information he gave to the Canadian authorities for that purpose.

[61] I now turn to consider the classified evidence on this issue. Since the disclosure of what personal information, if any, the Service shared with foreign agencies would be injurious to national security or the safety of persons, my analysis on this issue may be found in Section "B" of the Confidential Annex. I provide in the following paragraph a summary of my findings.

[62] I am satisfied that any information-sharing that took place in Mr. Mahjoub's case with foreign agencies was compliant with the statute and struck the appropriate balance between the public interest and Mr. Mahjoub's "residual" expectation of privacy.

[63] In summary, an individual has, at best, a residual privacy interest in information about that individual that is lawfully collected by the Service. Further, sharing of such information with foreign agencies under section 17 arrangements is constrained by the requirement that the Minister consult with DFAIT about a country before entering into such an arrangement. This informs the Service about the country conditions including the

human rights record of the country at issue. Paragraph 8(2)(*f*) of the *Privacy Act* and section 19 of the *CSIS Act* also provide parameters to protect the information by requiring a balancing of the interests and a determination that the public interest clearly outweighs any invasion of privacy. With these constraints in place, I am satisfied that, in Mr. Mahjoub's circumstances, the public interest in sharing the information outweighed the residual privacy interest of the individual.

[64] Moreover, upon reviewing the evidence on the record concerning Mr. Mahjoub's personal information that was shared, if any, with the foreign agencies, I am satisfied that his section 7 *Charter* right to privacy was not violated.

[65] I therefore conclude that section 17 of the *CSIS Act*, which permits intelligence-sharing arrangements with foreign agencies regardless of their human rights records, does not violate sections 7 and 8 of the *Charter*.

(c) *Are sections 21, 22, 23 and 24 of the* CSIS Act *unconstitutional for authorizing unreasonable search and seizure?*

[66] Sections 21, 22, 23 and 24 of the *CSIS Act* allow the Service to obtain warrants from the Federal Court in order to investigate threats to the security of Canada. Mr. Mahjoub alleges that these provisions are unconstitutional because they allow the Service to intercept solicitor-client communications.

[67] The Ministers maintain that the practice of intercepting solicitor-client communications as an incidental consequence of the interception of communications,

authorized by warrant under the *CSIS Act*, constitutes a long-standing exception to solicitor-client privilege based on the Federal Court of Appeal decision in *Atwal v. Canada*, [1988] 1 F.C. 107 (C.A.) [*Atwal*].

[68] For ease of reference, I reproduce below the impugned provisions 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.
(2) An application to a judge under subsection (1) shall be made in writing and be accompanied by an affidavit of the applicant deposing to the following matters, namely,	(2) La demande visée au paragraphe (1) est présentée par écrit et accompagnée de l'affidavit du demandeur portant sur les points suivants :
(*a*) the facts relied on to justify the belief, 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;	*a*) les faits sur lesquels le demandeur s'appuie pour avoir des motifs raisonnables de croire que le mandat est nécessaire aux fins visées au paragraphe (1);
(*b*) that other investigative procedures have been tried and have failed or why it appears that they are unlikely to succeed, that the urgency of the matter is such that it would be impractical to carry out the investigation using only other	*b*) le fait que d'autres méthodes d'enquête ont été essayées en vain, ou la raison pour laquelle elles semblent avoir peu de chances de succès, le fait que l'urgence de l'affaire est telle qu'il serait très difficile de mener

investigative procedures or that without a warrant under this section it is likely that information of importance with respect to the threat to the security of Canada or the performance of the duties and functions under section 16 referred to in paragraph (*a*) would not be obtained;

l'enquête sans mandat ou le fait que, sans mandat, il est probable que des informations importantes concernant les menaces ou les fonctions visées au paragraphe (1) ne pourraient être acquises;

…

[…]

(3) Notwithstanding any other law but subject to the *Statistics Act*, where the judge to whom an application under subsection (1) is made is satisfied of the matters referred to in paragraphs (2)(*a*) and (*b*) set out in the affidavit accompanying the application, the judge may issue a warrant authorizing the persons to whom it is directed to intercept any communication or obtain any information, record, document or thing and, for that purpose,

(3) Par dérogation à toute autre règle de droit mais sous réserve de la *Loi sur la statistique*, le juge à qui est présentée la demande visée au paragraphe (1) peut décerner le mandat s'il est convaincu de l'existence des faits mentionnés aux alinéas (2)*a*) et *b*) et dans l'affidavit qui accompagne la demande; le mandat autorise ses destinataires à intercepter des communications ou à acquérir des informations, documents ou objets. À cette fin, il peut autoriser aussi, de leur part :

(*a*) to enter any place or open or obtain access to any thing;

a) l'accès à un lieu ou un objet ou l'ouverture d'un objet;

(*b*) to search for, remove or return, or examine, take extracts from or make copies of or record in any other manner the information, record, document or thing; or

b) la recherche, l'enlèvement ou la remise en place de tout document ou objet, leur examen, le prélèvement des informations qui s'y trouvent, ainsi que leur enregistrement et l'établissement de copies ou d'extraits par tout procédé;

(*c*) to install, maintain or remove any thing.

c) l'installation, l'entretien et l'enlèvement d'objets.

(4) There shall be specified in a warrant issued under subsection (3)

(*a*) the type of communication authorized to be intercepted, the type of information, records, documents or things authorized to be obtained and the powers referred to in paragraphs (3)(*a*) to (*c*) authorized to be exercised for that purpose;

(*b*) the identity of the person, if known, whose communication is to be intercepted or who has possession of the information, record, document or thing to be obtained;

(*c*) the persons or classes of persons to whom the warrant is directed;

(*d*) a general description of the place where the warrant may be executed, if a general description of that place can be given;

(*e*) the period for which the warrant is in force; and

(*f*) such terms and conditions as the judge considers advisable in the public interest.

…

22. On application in writing to a judge for the renewal of a warrant issued under subsection 21(3) made by a person entitled to apply for

(4) Le mandat décerné en vertu du paragraphe (3) porte les indications suivantes :

a) les catégories de communications dont l'interception, les catégories d'informations, de documents ou d'objets dont l'acquisition, ou les pouvoirs visés aux alinéas (3)*a*) à *c*) dont l'exercice, sont autorisés;

b) l'identité de la personne, si elle est connue, dont les communications sont à intercepter ou qui est en possession des informations, documents ou objets à acquérir;

c) les personnes ou catégories de personnes destinataires du mandat;

d) si possible, une description générale du lieu où le mandat peut être exécuté;

e) la durée de validité du mandat;

f) les conditions que le juge estime indiquées dans l'intérêt public.

[…]

22. Sur la demande écrite, approuvée par le ministre, que lui en fait une personne autorisée à demander le mandat visé au paragraphe

such a warrant after having obtained the approval of the Minister, the judge may, from time to time, renew the warrant for a period not exceeding the period for which the warrant may be issued pursuant to subsection 21(5**)**

21(3), le juge peut le renouveler, pour une période n'excédant pas celle pour laquelle ce mandat peut être décerné en vertu du paragraphe 21(5)

…

[…]

23. (1) On application in writing by the Director or any employee designated by the Minister for the purpose, a judge may, if the judge thinks fit, issue a warrant authorizing the persons to whom the warrant is directed to remove from any place any thing installed pursuant to a warrant issued under subsection 21(3)

23. (1) Sur la demande écrite que lui en fait le directeur ou un employé désigné à cette fin par le ministre, le juge peut, s'il l'estime indiqué, décerner un mandat autorisant ses destinataires à enlever un objet d'un lieu où il avait été installé en conformité avec un mandat décerné en vertu du paragraphe 21(3)

…

[…]

24. Notwithstanding any other law, a warrant issued under section 21 or 23

24. Par dérogation à toute autre règle de droit, le mandat décerné en vertu des articles 21 ou 23 :

(*a*) authorizes every person or person included in a class of persons to whom the warrant is directed,

a) autorise ses destinataires, en tant que tels ou au titre de leur appartenance à une catégorie donnée :

(i) in the case of a warrant issued under section 21, to exercise the powers specified in the warrant for the purpose of intercepting communications of the type specified therein or obtaining information, records, documents or things of the type specified therein, or

(i) dans le cas d'un mandat décerné en vertu de l'article 21, à employer les moyens qui y sont indiqués pour effectuer l'interception ou l'acquisition qui y est indiquée,

(ii) in the case of a warrant issued under section 23, to execute the warrant; and	(ii) dans le cas d'un mandat décerné en vertu de l'article 23, à exécuter le mandat;
(*b*) authorizes any other person to assist a person who that other person believes on reasonable grounds is acting in accordance with such a warrant.	*b*) autorise quiconque à prêter assistance à une personne qu'il a des motifs raisonnables de croire habilitée par le mandat.

[69] The Federal Court of Appeal in *Atwal* finds that the *CSIS Act* warrant regime described in these provisions is constitutional following a challenge to certain warrants in the context of a criminal proceeding. The Court of Appeal also finds that when specifically authorized by a warrant, the Service may intercept solicitor-client communications for the purposes of ascertaining whether there is a threat to national security. In addition, the exception to solicitor-client privilege described in *Atwal* is confined to the limits of section 12 of the *CSIS Act*, which requires the acquisition and retention of the information to be "strictly necessary" to investigate a security threat. Moreover, the potential for incidental interception of solicitor-client communications is a preoccupation of the Court in the process of judicial approval due to the unique status of solicitor-client privilege as a principle of fundamental justice in Canadian law **(***Lavallee, Rackel & Heintz v. Canada (Attorney General)*, 2002 SCC 61 [*Lavallee*] at paragraph 21).

[70] Mr. Mahjoub argues that *Atwal* is not good law. He contends that the Federal Court of Appeal was bound to follow the earlier Supreme Court of Canada decisions in *Descoteaux et al. v. Mierzwinski*, [1982] 1 S.C.R. 860 [*Descoteaux*] and *Solosky v. The Queen*, [1980] 1 S.C.R. 821 [*Solosky*]. In deciding as it did in *Atwal*, Mr. Mahjoub

contends that the Federal Court of Appeal was purporting to overrule the Supreme Court jurisprudence.

[71] In order to address the argument raised by Mr. Mahjoub, it is necessary to review these decisions in some detail.

[72] *Atwal* is an appeal of a decision of a designated judge to refuse to rescind a *CSIS Act* warrant. Previously, the designated judge issued a warrant pursuant to subsection 21(1) of the *CSIS Act* against Mr. Atwal to search and seize documents and intercept communications, the fruits of which were used to charge Mr. Atwal with conspiracy to commit murder. *Atwal* directly addresses the issue of solicitor-client privileged communications. At page 123 of the decision, the Court of Appeal notes that the appellant raised the issue of the warrant's non-compliance with section 21 of the *CSIS Act* since "it authorizes seizure and interception of privileged solicitor-client communications."

[73] At pages 128-133, the Federal Court of Appeal explained that a section 21 warrant may authorize the interception of solicitor-client communications. The Court distinguished a treatise on the law of electronic surveillance which proposes limits on surveillance to protect privileged information after a criminal charge is laid. The Court of Appeal noted that the situations are not analogous because the appellant was not charged while the warrant was in effect. The Court also dispensed with the appellant's concern that notwithstanding the requirements of the warrant condition forbidding disclosure, a person with knowledge

thereof, for example the Director or a translator, would, nevertheless, be compellable as a witness to testify as to its content. The Court reasoned as follows:

> In so arguing, the appellant accords no force to the mandatory language of condition 3 forbidding such disclosure and the readiness of the courts to exclude evidence whose admission would tend to bring into disrepute the administration of justice. I cannot conceive that the apprehended situation could actually arise.

[74] At page 130, the Court of Appeal acknowledged the requirement posited by the Supreme Court in *Descoteaux*, that solicitor-client privilege must now be examined as a substantive rule of law and not a rule of evidence as it once was. Citing *Descoteaux* at page 875, the Court of Appeal reproduced the Supreme Court's formulation of the substantive rule:

> 1. The confidentiality of communications between solicitor and client may be raised in any circumstances where such communications are likely to be disclosed without the client's consent.
>
> 2. Unless the law provides otherwise, when and to the extent that the legitimate exercise of a right would interfere with another person's right to have his communications with his lawyer kept confidential, the resulting conflict should be resolved in favour of protecting the confidentiality.
>
> 3. When the law gives someone the authority to do something which, in the circumstances of the case, might interfere with that confidentiality, the decision to do so and the choice of means of exercising that authority should be determined with a view to not interfering with it except to the extent absolutely necessary in order to achieve the ends sought by the enabling legislation.
>
> 4. Acts providing otherwise in situations under paragraph 2 and enabling legislation referred to in paragraph 3 must be interpreted restrictively.

[75] The Court of Appeal addressed items iii and iv of the above-cited requirements at page 130 of its decision as follows:

> Subsection 21(3) authorizes the judge to issue a warrant "to intercept any communication". Given that the confidential character of such communications when electronically intercepted cannot possibly be ascertained before they are monitored, the authority of subsection 21(3) simply cannot be interpreted so as to preclude their initial interception. In my view, conditions 2 and 3 set forth in the warrant do meet the requirement that the confidentiality of solicitor-client communications be interfered with only to the extent absolutely necessary to achieve the objects of the Act. The relevant objects are stated in section 12.

[76] In my view, *Atwal* does not conflict with *Descoteaux* or take it out of context as alleged by Mr. Mahjoub. It adapts the requirements of *Descoteaux* to the national security context. *Descoteaux* was not decided in the national security context. The case involved a search of documents at a legal aid clinic, including an individual's application for legal aid, for which a warrant was issued on reasonable grounds to believe that individual had committed the indictable offence of underreporting income in order to be eligible for legal aid.

[77] At pages 872-873 of its reasons in *Descoteaux*, the Supreme Court adopted the following statement in Wigmore on Evidence as a good summary of the substantive conditions precedent to the existence of the right of the lawyer's client to confidentiality:

> Where legal advice of any kind is sought from a professional legal adviser in his capacity as such, the communications relating to that purpose, made in confidence by the client, are at his instance permanently protected from disclosure by himself or by the legal adviser, except the protection be waived.

[78] The Court went on to recognize exceptions to the rule. It stated at page 873:

> There are exceptions. It is not sufficient to speak to a lawyer or one of his associates for everything to become confidential from that point on. The communication must be made to the lawyer or his assistants in their professional capacity; the relationship must be a professional one at the exact moment of the communication. Communications made in order to facilitate the commission of a crime or fraud will not be confidential either, regardless of whether or not the lawyer is acting in good faith.

[79] The Supreme Court gave no guidance here as to applicable process to determine if the solicitor-client communication was made in the lawyer or assistants' professional capacity or to facilitate the commission of a crime or fraud. In fact, at page 896 the Supreme Court stated "that the procedure will vary from one case to another." Mr. Mahjoub contends that the Supreme Court provides such guidance in *Solosky*. *Solosky* at pages 841-842 establishes that there must be "reasonable and probable grounds to believe" that the communications are not solicitor-client privileged before the contents can be read or heard.

[80] *Solosky* involved the interception of an inmate's mail. The *Penitentiary Act*, R.S.C. 1970, c. P-6, allowed inmates' mail to be intercepted if those inmates were considered a threat "to the safety and security of the institution", and the Supreme Court interpreted the regulation to mean that "the envelope be subject to opening and examination to the minimum extent necessary to establish whether it is properly the subject of solicitor-client privilege." *Solosky* imposes a greater restriction on officials intercepting solicitor-client communications than *Atwal*.

[81] T

he circumstances of section 21 warrants are far different and involve the investigation of a threat to the security of Canada, in a context that pre-dates any legal proceeding, and when regular contact with legal counsel is not expected for legal advice. In my view, *Solosky* can therefore be distinguished on its facts. *Atwal* was decided in the national security context and reflects the state of the law in Canada concerning section 21 warrants authorizing interception of solicitor-client communications to which this Court is bound. My determination finds support in *Corp. of Canadian Civil Liberties Assn. v. Canada (Attorney General)* (1998), 40 O.R. (3d) 489, at paragraphs 38, 78, and 90-91 (C.A.). In that case, on a similar constitutional challenge, section 21 warrants were found to be constitutional, and the Court expressly relies on *Atwal* as the leading case. Leave to appeal to the Supreme Court of Canada was refused.

[82] While I find *Atwal* to be binding in the circumstances, that is not to say that *Solosky* does not provide guidance relating to appropriate restrictions on solicitor-client intercepts after the issuance of the security certificate and the arrest of the named person. It is then difficult to distinguish Mr. Mahjoub's circumstances since he was an inmate. The censorship of penitentiary correspondence is reasonably analogous to the interception of Mr. Mahjoub's communications while incarcerated, and in my mind more analogous than the facts of *Atwal*.

[83] The jurisprudence appears to require a more stringent standard for exceptions to solicitor-client privilege when the information is sought for the purpose of acquiring evidence for legal proceedings. See: *Lavallee* and *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, 2008 SCC 44 [*Blood Tribe*]. I note that *Solosky* was cited with approval in *Lavallee* as the leading case on the issue in its circumstances. In *Solosky*, the standard is articulated as follows at pages 841-842:

> [The] "minimum extent necessary to establish whether it is properly the subject of solicitor-client privilege" should be interpreted in such a manner that:
> (i) the contents of an envelope may be inspected for contraband;
> (ii) in limited circumstances, the communication may be read to ensure that it, in fact, contains a confidential communication between a solicitor and client written for the purpose of seeking or giving legal advice;
> (iii) the letter should only be read if there are reasonable and probable grounds for believing the contrary, and then only to the extent necessary to determine the bona fides of the communication;
> (iv) the authorized penitentiary official who examines the envelope, upon ascertaining that the envelope contains nothing in breach of security, is under a duty at law to maintain the confidentiality of the communication.

[84] In *Almrei (Re)*, 2008 FC 1216, Justice Mosley addressed a constitutional challenge to the *IRPA* based on an alleged breach to solicitor-client privilege. He observed the following on the issue at paragraphs 60 and 61of his reasons:

> [60] Despite its importance, solicitor-client privilege is not absolute: *R. v. McClure*, [2001] 1 S.C.R. 445, at paragraphs 34-35. The case law relied upon by the named persons to buttress the importance of the solicitor-client privilege does not exclude its possible breach for reasons of necessity: *Canada (Privacy* Commissioner*) v. Blood Tribe Department of Health*, 2008 SCC 44, [2008] 2 S.C.R. 574, at paragraphs 17 and 22; *Lavallee, Rackel & Heintz v. Canada (Attorney General); White, Ottenheimer & Baker v. Canada*

> *(Attorney General); R. v. Fink*, 2002 SCC 61, [2002] 3 S.C.R. 209, at paragraph 36; *Smith v. Jones*, [1999] 1 S.C.R. 455, at paragraph 57.
>
> [61] Avoiding injury to national security, which can include the risks of inadvertent disclosure, may constitute a necessity that warrants piercing the privilege in as minimal ways as the circumstances dictate. This should not be decided in a factual vacuum.

[85] To conclude, I am satisfied that *Atwal* has not been overruled and is binding on this Court. It creates a national security exception to solicitor-client privilege in the narrow context of a prospective CSIS investigation of a national security threat authorized by a section 21 warrant.

[86] Once an individual is detained and/or legal proceedings are initiated, it is my view that the narrower exception to solicitor-client privilege found in *Solosky* applies to any warrants issued. While the interest in protecting national security and the security of the detention institution is still present, the warrant must require that once a communication is identified as one between solicitor and client, CSIS must have reasonable and probable grounds for believing that it is not a legitimate solicitor-client communication or that it pertains to imminent danger before the interception can go any further.

[87] I am satisfied that *Atwal* has not been overruled and as such I am bound by its determination. The constitutional challenge raised in this case relating to the interception of solicitor-client communications authorized by section 21 warrants, has been decided by *Atwal*. Section 21 of the *CSIS Act* is not unconstitutional simply because section 21

warrants may authorize the incidental interception of solicitor-client communications for the purposes of a prospective investigation.

Conclusion on the first issue

[88] On the basis of the challenges submitted by Mr. Mahjoub and the facts of this case, I find that the impugned provisions of the *CSIS Act* infringe neither section 7, section 8 nor any other section of the *Charter*.

[89] The term "threats to the security of Canada" is adequately defined in section 2 of the *CSIS Act* to provide notice to the citizen of what kind of activities will be investigated and limits on the Service's discretion to investigate activities. Parliament did not contemplate that section 12 would authorize unreasonable searches and seizures when privacy rights were engaged. Instead, intrusive searches and seizures were to be authorized by section 21 warrants. Section 6 does not engage Mr. Mahjoub's rights and cannot be impugned by allegations attacking the constitutionality of the Service's policies developed thereunder. Arrangements with foreign agencies established by the authority of section 17 do not infringe Mr. Mahjoub's rights, even if they entail sharing the personal information in the possession of the Service as intelligence. The public interest in sharing the information to further the mandate of CSIS is greater than the "residual" privacy interest that Mr. Mahjoub has in the information. Lastly, sections 21-24 of the Act do not permit unreasonable searches and seizures simply because they allow the Federal Court to authorize the interception of solicitor-client communications. Prior to

the commencement of any legal proceedings against a target, it may be necessary to incidentally intercept such communications in the interests of national security.

2. *Can the lawfulness of the section 21 warrants be challenged?*

[90] The Ministers argue, as a preliminary matter, that Mr. Mahjoub is mounting an impermissible collateral attack on the validity of the warrants in his challenge to the lawfulness of the section 21 warrants in these proceedings.

[91] Mr. Mahjoub raises two preliminary issues relating to the extent to which the warrants can be challenged. First, he alleges that the evidence obtained pursuant to the section 21 warrants is *a priori* inadmissible because it was obtained as a result of the previous *IRPA* regime that was declared unconstitutional in *Charkaoui I*. Second, he alleges that he is unable to effectively make his challenge to the warrants because the full text of the warrants and the supporting affidavits has not been disclosed to him, infringing his right to full answer and defence. In the alternative, he argues that the Court should be restricted to considering the lawfulness of the warrants on the basis of the information that was disclosed to him, without regard to the information that does not appear in the summaries, akin to the process used when an accused challenges a *Criminal Code* warrant.

(a) *Does the doctrine of collateral attack preclude challenge to the validity of the section 21 warrants in the context of determining the admissibility of evidence pursuant to section 24 of the* Charter *in a security certificate proceeding?*

[92] The Ministers rely on the decision *Wilson v. The Queen*, [1983] 2 S.C.R. 594 [*Wilson*], in support of their submission that this challenge to the warrants is a collateral attack on the Court's decision to issue warrants *ex parte* pursuant to section 21 of the *CSIS Act*. They argue that Mr. Mahjoub cannot "reach back" and challenge the warrants in attempting to exclude the evidence obtained under the warrants' authority.

[93] *Wilson* at page 607 states that "[s]ince no right of appeal is given from the granting of an authorization and since prerogative relief by *certiorari* would not appear to be applicable (there being no question of jurisdiction), any application for review of an authorization must, in my opinion, be made to the court that made it." At page 608, the Supreme Court adds that it is not always "practical or possible to apply for a review to the same judge who made the order…another judge of the same court can review an *ex parte* order", but it cautions that "[t]he reviewing judge must not substitute his discretion for that of the authorizing judge" and only permits the reviewing court to disturb the warrant authorization "if the facts upon which the authorization was granted are found to be different from the facts proved on the *ex parte* review…".

[94] *Wilson* also provides a useful definition of collateral attack at page 599: "a collateral attack may be described as an attack made in proceedings other than those whose specific object is the reversal, variation, or nullification of the order or judgment." The Supreme Court only allows for a collateral attack "in cases where there has been a defect on the face of the authorization or fraud" (at page 604).

[95] In my view, Mr. Mahjoub's challenge to the section 21 warrants, particularly to the admissibility of the evidence obtained as a result of those warrants, does not fit within the above-cited definition of collateral attack. Although Mr. Mahjoub has mislabelled his challenge as an application pursuant to paragraph 399(1)(*a*) of the *Federal Courts Rules* and section 18 of the *Federal Courts Act*, I am satisfied the application is essentially a subsection 24(2) application to exclude evidence on the basis that it was obtained in violation of Mr. Mahjoub's *Charter* rights and that its admission will bring the administration of justice into disrepute.

[96] The main issue that *Wilson* raises is the issue of appropriate forum. In *Wilson*, a provincial court refused to accept the authorization of a superior court. The Supreme Court confirmed that a review of the authorization had to be conducted by the court that made it.

[97] The only restriction that the Supreme Court places on this review is that "[t]he reviewing judge must not substitute his discretion for that of the authorizing judge. Only if the facts upon which the authorization was granted are found to be different from the facts proved on the *ex parte* review should the authorization be disturbed." Finally, at page 609, Justice McIntyre accepts the possibility that "rather than incurring extra expense and needless delay by instituting completely separate proceedings," if the trial judge happens to be of the same court as the judge who made the authorization, an application could be made directly to him or her "in his capacity as a judge of the court that made the original order…".

[98] The latter scenario is analogous to the situation in this case. This is a common occurrence in a criminal proceeding. In fact, *R. v. Garofoli*, [1990] 2 S.C.R. 1421 [*Garofoli*], deals with this issue in a more pertinent way than *Wilson* at pages 1448 and 1449:

> In my opinion, when it is asserted by an accused that a wiretap infringes s. 8, an appropriate review is incompatible with the restrictions of *Wilson*. The judge conducting the review must hear evidence and submissions as to whether the interception constitutes an unreasonable search or seizure. Inasmuch as it is an issue as to the admissibility of evidence, it may be raised at trial. Under s. 24 of the *Charter*, the trial judge is a court of competent jurisdiction.

[99] These comments are not restricted to mere access to the wiretap packet as the Ministers contend.

[100] Moreover, the majority in *R. v. Litchfield*, [1993] 4 S.C.R. 333 at page 349, held that the doctrine of collateral attack is "not intended to immunize court orders from review." It is almost unheard of for a challenge to a warrant issued pursuant to section 21 of the *CSIS Act* to occur in any circumstances other than in a proceeding in which the fruits of that warrant are being tendered as evidence, such as a criminal proceeding like *R. v. Ahmad*, 2011 SCC 6 or *Atwal*, or an immigration proceeding like this case. It is the nature of the warrants that they are for the most part unknown to their targets. In the circumstances where the possibility of effective challenge through normal review and appeal routes is unrealistic, it is even more important that the rule against collateral attack

be applied flexibly (*Dagenais v. Canadian Broadcasting Corp.*, [1994] 3 S.C.R. 835 at page 871).

[101] To accept the Ministers' position would be to immunize section 21 warrants from review, and it would deprive Mr. Mahjoub of his ability to make use of section 24 of the *Charter* to exclude evidence that he alleges was unconstitutionally obtained due to the invalidity of the warrants. I therefore reject the Ministers' argument that this application amounts to a collateral attack.

[102] I now turn to the issues raised by Mr. Mahjoub.

(b) *Is the evidence obtained pursuant to the section 21 warrants inadmissible because Charkaoui I declared the previous* IRPA *regime, which was the law at the time the evidence was collected, unconstitutional?*

[103] I see no merit to Mr. Mahjoub's argument that the evidence collected under the authority of warrants issued pursuant to section 21 of the *CSIS Act* should be inadmissible because the previous *IRPA* regime was found to be unconstitutional. While in *Charkaoui I* the Supreme Court dealt with a challenge to the *IRPA*, the warrants at issue were issued under section 21 of the *CSIS Act*, different legislation entirely. To date, the *CSIS Act* has been found to be constitutional by the Federal Court of Appeal in *Atwal*. In *Charkaoui I*, the Supreme Court makes no comment on the constitutionality of *CSIS Act* warrants. As a result, I reject Mr. Mahjoub's argument.

(c) *Does the non-disclosure of the confidential section 21 warrants and affidavits in support of the warrants to Mr. Mahjoub violate Mr. Mahjoub's right to full answer and defence?*

[104] Mr. Mahjoub submits that he cannot mount an effective challenge to the warrants without disclosure of the full text of the section 21 warrants and the supporting affidavits that were before the issuing designated judge. He argues that this situation violates his right to full answer and defence, and that the violation must be remedied by excluding the evidence obtained under the authority of the warrants.

[105] The right of an accused person to full answer and defence in the criminal context is not directly applicable to a named person in security certificate proceedings. The Supreme Court of Canada and the Federal Court of Appeal have characterized the right of the named person as a right to know the case to meet and to respond to that case, which exists within the broader context of the right to a fair trial. *Charkaoui II* raises the issue of "full answer and defence," explaining it specifically in the criminal context of *R. v. Stinchcombe*, [1991] 3 S.C.R. 326, beginning at paragraph 48. Section (b) of the decision, starting at paragraph 50, is titled: "*Distinguishing the Context of the Security Certificate*". Paragraph 50 explains the differences and similarities in context:

> The principles governing the disclosure of evidence are well established in criminal law, but the proceeding in which the Federal Court determines whether a security certificate is reasonable takes place in a context different from that of a criminal trial. No charges are laid against the person named in the certificate. Instead, the ministers seek to expel the named person from Canada on grounds of prevention or public safety. However, the serious consequences of the procedure on the liberty and security of the named person bring interests protected by s. 7 of the *Charter* into play. A form of disclosure of all the information that goes beyond the mere summaries which are currently provided by CSIS to the ministers and the designated judge is required to

> protect the fundamental rights affected by the security certificate procedure.

[106] At paragraph 51, the Supreme Court cites *Blencoe v. British Columbia (Human Rights Commission)*, 2000 SCC 44 at paragraph 88: "[t]his Court has often cautioned against the direct application of criminal justice standards in the administrative law area." The Supreme Court proceeds to explain the extent of the duty to disclose at paragraph 56:

> In *La* (at para. 20), this Court confirmed that the duty to disclose is included in the rights protected by s. 7. Similarly, in *Ruby v. Canada (Solicitor General)*, 2002 SCC 75, [2002] 4 S.C.R. 3, 2002 SCC 75, at paras. 39-40, the Court stressed the importance of adopting a contextual approach in assessing the rules of natural justice and the degree of procedural fairness to which an individual is entitled. In our view, the issuance of a certificate and the consequences thereof, such as detention, demand great respect for the named person's right to procedural fairness. In this context, procedural fairness includes a procedure for verifying the evidence adduced against him or her. It also includes the disclosure of the evidence to the named person, in a manner and within limits that are consistent with legitimate public safety interests. [Emphasis added].

[107] It is plain that the Supreme Court does not import "full answer and defence" into the security certificate context. At paragraph 58, the Supreme Court instead invokes an "expanded right to procedural fairness, one which requires the disclosure of information…" and a mechanism for verifying evidence adduced against the named person.

[108] This right is explained more thoroughly in *Charkaoui I*, which states at paragraph 20, that "[s]ection 7 of the *Charter* requires not a particular type of process, but a fair

process having regard to the nature of the proceedings and the interests at stake…". At paragraph 24, the Supreme Court states that "[f]ull disclosure of the information relied on may not be possible," and at paragraph 27, it explains "[t]he principles of fundamental justice cannot be reduced to the point where they cease to provide the protection of due process … The protection may not be as complete as in a case where national security constraints do not operate. But to satisfy section 7, meaningful and substantial protection there must be." Finally, at paragraph 29 of *Charkaoui I*, the Supreme Court mentions the essentials of the section 7 rights to due process when extended detention and potential deportation is involved: "it entails the *right to know the case put against one*, and the *right to answer that case*. Precisely how these requirements are met will vary with the context."

[109] Further, at paragraph 71 of *Harkat v. Canada (Citizenship and Immigration)*, 2012 FCA 122 [*Harkat*], the Federal Court of Appeal explains the section 7 rights at stake from the perspective of disclosure in security certificate proceedings:

> The principles of fundamental justice have been discussed by the Supreme Court. In *Charkaoui* #1, the Court "recognized that national security considerations can limit the extent of disclosure of information to the affected individual" and that protection of investigative techniques and police sources as well as the safeguard of confidential public security documents and the maintenance of foreign confidences are "societal concerns [which] formed part of the relevant context for determining the scope of the applicable principles of fundamental justice". Nonetheless, the fundamental principles of justice command that the affected person be given a fair hearing. In other words, the affected person must not only be informed of the case to meet, but also be given an opportunity to meet that case. [Emphasis added]

[110] In determining the constitutionality of the provision requiring the Federal Court to provide the named person with summaries at paragraph 82, the Federal Court of Appeal continues to employ the same language as *Charkaoui I* and *Charkaoui II*, the language of knowing the case to meet and being able to answer that case. Nowhere in the Federal Court of Appeal's decision in *Harkat* does one find the language of "full answer and defence" except to explain a criminal case (at paragraph 111).

[111] While in many respects the right to know the case to meet and to respond to the case resembles the right to full answer and defence, an important distinction between them is that the right to disclosure or a remedy for non-disclosure is different, in the sense that in security certificate cases the right is not as absolute. In *Charkaoui I*, the Supreme Court observes at paragraph 61 that a "substantial substitute" for disclosure would be sufficient to meet the right to a fair trial in security certificate proceedings.

[112] As explained in the *Constitutional Decision* at paragraphs 83-84, the Federal Court of Appeal in *Harkat* finds the special advocates regime, coupled with the disclosure of summaries to Mr. Mahjoub, in the current incarnation of the *IRPA* to be a substantial substitute for disclosure. The Federal Court of Appeal concludes at paragraph 116 "that paragraph 85.4(2) and section 85.5 of the Act have built in the flexibility necessary to ensure the fairness of the process and the protection of national security and the safety of any person." It elaborates at paragraph 119:

> The revised Act provides the judge with the necessary tools to ensure a fair process. With the assistance of the special advocates acting on behalf of the appellant, the judge is vested with the necessary powers at common law and under the *Charter* and the

> Act to satisfy the fairness requirement of section 7 of the *Charter*. He possesses the power to order disclosure of information, authorize additional communications, remedy a failure to disclose and grant a just and appropriate remedy under subsection 24(1) of the *Charter* where a breach of procedural fairness has occurred. He can take preemptive action to prevent a violation of a named person's right to liberty and security of the person. All of these factors, coupled with the *Charkaoui* #2 disclosure, are a sufficient substitute for full disclosure. [Emphasis added]

[113] The Court is bound by this finding.

[114] The Special Advocates were provided disclosure of the section 21 warrants and supporting affidavits. Mr. Mahjoub has been given a detailed summary of these warrants and supporting affidavits sufficient for him to be reasonably informed of them (see the Court's October 5, 2010 Order). The specifics of the warrants must be kept confidential because their disclosure would be injurious to national security or the safety of any person. However, Mr. Mahjoub has been able to raise general challenges to the lawfulness of the warrants and the searches and seizures performed by the Service ostensibly under the authority of those warrants. The Special Advocates have been able to support these challenges *in camera* by making targeted submissions dealing with the confidential specifics of the warrants and supporting affidavits. The Special Advocates had the opportunity to raise any additional challenges to the warrants and the Service's searches and seizures based on the confidential specifics that had not been raised by Mr. Mahjoub.

[115] In my view, Mr. Mahjoub's right to know the case to meet and to respond to that case has been satisfied by this process. I am of the opinion that given the particular role of the Special Advocates and their involvement in the proceeding, and the summaries of the warrant materials provided to Mr. Mahjoub, that he was in a position to mount an effective challenge to the section 21 warrants. This is so even though not all of the warrant materials were available to Mr. Mahjoub for national security reasons.

(d) *In the context of a challenge to section 21 warrants in a security certificate proceeding, can the Court consider the confidential affidavits, or must the Court restrict its consideration to the summary of the affidavits disclosed to Mr. Mahjoub?*

[116] I reject Mr. Mahjoub's alternative submission that the Court must restrict its consideration to the disclosed summaries of the warrants and the supporting affidavits as is the practice in criminal proceedings. He argues that in criminal proceedings when an accused person challenges a warrant and gains access to, for example, the wiretap packet, the Crown may claim public interest privilege over portions of the packet and redact them from the disclosed contents of the packet. In considering the validity of the wiretap, the Court must restrict itself to what is disclosed to the accused person. In my view, such a restriction is not required to protect the fairness of these proceedings.

[117] Even in the criminal context, the Supreme Court has made allowances for the judge to rely on undisclosed information if an adequate summary that respects the accused's right to full answer and defence can be provided to the accused (*Garofoli* at page 1461). In addition, there are two elements of the criminal process that distinguish it from the security certificate process. First, in the criminal process, the accused has a right

to full answer and defence, and if there is less than complete disclosure of relevant information from the Crown, the deficiency in disclosure must have a remedy, not a substitute. Second, and most importantly, Mr. Mahjoub's Special Advocates have received full disclosure of the warrants and supporting affidavits. They are in a position to represent Mr. Mahjoub's interests *in camera* and to make use of the information that cannot be disclosed to Mr. Mahjoub. Further, Mr. Mahjoub is entitled to instruct the Special Advocates at any time. While I agree with Mr. Mahjoub's submission that he is unable to tell from the summaries whether or not the warrants complied with the *CSIS Act*, the Special Advocates can and have made submissions *in camera* on the issue of compliance with the *CSIS Act* with the specifics of the warrants and supporting affidavits at their disposal.

[118] The above-noted differences between criminal and security certificate proceedings justify different approaches to disclosure when warrants are challenged. In a criminal proceeding, the accused does not have access to information that is subject to public interest privilege, and for this reason the Court usually restricts itself to what is disclosed to the accused. The restriction is not warranted in the context of security certificate proceedings. Since the Special Advocates have access to the classified materials, including the warrants and their supporting affidavits, it would be inconsistent not to allow the Court access to such material in deciding the issue. There is no basis for restricting the record to what is disclosed to the named person. As stated above, the Special Advocates can protect the interests of the named person with respect to the classified information.

[119] In the circumstances, the Court is in a better position to decide the lawfulness of the warrants that are subject to challenge if it considers the classified record and not just the public summary. As stated above, given the particular role of the Special Advocates, there is no basis to restrict the record in the manner suggested by Mr. Mahjoub. His argument is consequently rejected.

3. *Are the section 21 warrants unlawful?*

[120] Mr. Mahjoub makes several substantive challenges to the warrants, including that they are invalid because of the information derived from torture in the supporting affidavits, the Service's breach of the duty of full, fair and frank disclosure to the designated judge who issued the warrants, the absence of any indication that the Service complied with the requirements of subsections 21(1) and paragraphs 21(2)(*a*) to (*g*) of the *CSIS Act*, and the warrants' apparent authorization of the Service to intercept solicitor-client privileged communications.

[121] I will deal with each of these challenges in turn.

(a) *The presence of information derived from torture in the supporting affidavits?*

[122] While I have rejected the Ministers' submission that the Court's August 31, 2010 Order disposes of this entire application, I am satisfied that the Court's June 9, 2010 and August 31, 2010 Reasons for Order combined dispose of this particular argument. This issue was before the Court in the subsection 83(1.1) motion and the Court pronounced

upon it. Mr. Mahjoub cannot re-litigate this issue. The relevant portions of paragraphs 60-73 of the August 31, 2010 Order read as follows:

> [60] Having identified the information in the affidavit that on reasonable grounds to believe was obtained from torture, I now turn to the question of whether, but for this information, the warrant would have been issued…
>
> [61] The evidence does not establish that there are reasonable grounds to believe that the above information was obtained by the use of torture or CIDT. Further, I am of the view that the said information justifies, on reasonable grounds, the belief that a warrant for the interception of Mr. Mahjoub was required for the Service to investigate a threat to the security of Canada pursuant to the requirements of section 21 of the CSIS Act. It follows, in my view that the warrant would have issued absent the information obtained from [redacted] interrogation. Consequently, the information obtained and relied on by the Ministers from the intercepted communications, obtained as a result of supplementary Warrant [redacted] is admissible.
>
> [62] I now turn to the information obtained from intercepted communications authorized by Warrant [redacted]…
>
> …
>
> [64] Other than the information identified as having been obtained from the interrogation of [redacted], the affidavit in support of the Warrant [redacted] also contains other information, which is relied on to justify the interception powers requested with respect to Mr. Mahjoub…
>
> …
>
> [66] I am of the view that he information in the supporting affidavit, not sourced from [redacted] interrogation, was sufficient to justify on reasonable grounds the belief that the warrant powers to intercept Mr. Mahjoub's private communications were required …Consequently, the information obtained and relied on by the Ministers from the intercepted communications obtained as a result of the Warrant [redacted] is admissible.
>
> [67] I now turn to the information obtained from intercepted communications authorized by Warrant [redacted]…

…

> [73] I am also of the view that the facts relied on in the supporting affidavit to Warrant [redacted], not sourced from the interrogation of [redacted] nor from the convictions from the Returnees of Albania trial, were sufficient to support on reasonable grounds the belief that a Warrant [redacted], and in particular the warrant power to intercept Mr. Mahjoub's private communications, was required…It follows that the warrant would have issued absent the information obtained from [redacted] interrogation and from the convictions of the Returnees of Albania trial. Consequently, the information obtained and relied on by the Ministers from the interceptions obtained as a result of the Warrant [redacted] is admissible.

[123] I have therefore already decided that the warrants could have issued but for the information for which there are reasonable grounds to believe it was obtained by torture or cruel, inhuman or degrading treatment, and the evidence obtained as a result of the warrants is not inadmissible for this reason.

(b) *CSIS's breach of the duty of full, fair and frank disclosure by presenting misleading affidavits to the designated judge that also omitted exculpatory information?*

[124] Mr. Mahjoub submits that in seeking an *ex parte* section 21 warrant under the *CSIS Act*, the Service owed a duty to provide the designated judge with "full, fair and frank disclosure." The Ministers, while preferring to call the duty a "duty of candour," are essentially in agreement. In general, parties bringing *ex parte* applications are expected to provide the court with full, fair and frank disclosure (*Ruby v. Canada (Solicitor General)*, 2002 SCC 75 [*Ruby*] at paragraph 47). See also *R. v. Morelli*, 2010 SCC 8 [*Morelli*] at paragraph 44. The Supreme Court in *Ruby* explains that "[t]he evidence presented [*ex parte* by government agencies] must be complete and thorough

and no relevant information adverse to the interest of that party may be withheld" (at paragraph 27).

[125] Mr. Mahjoub argues that the Service breached the duty of candour by failing to include in its affidavits submitted to the designated judge in support of the warrants exculpatory evidence as well as including therein intentionally misleading statements.

[126] Mr. Mahjoub alleges that the following exculpatory information is missing from the affidavits:

a. the controversy surrounding the existence of the Vanguards of Conquest;

b. details of Mr. Mahjoub's version of events submitted to the Immigration and Refugee Board in his Personal Information Form (PIF);

c. Mr. Jaballah's quashed security certificate, and

d. the omissions described by Professors Wark and Gerges**,** namely

i. how Mr. Mahjoub joined Al Jihad or the Vanguards of Conquest and rose in the ranks to a leadership position;

ii. how Mr. Mahjoub was involved in the operations of these groups;

iii. the aid that Al Jihad provided to the United States in the Afghan-Soviet War;

iv. the recent de-radicalization of Islamist politics;

v. the opposition within Al Jihad to Osama Bin Laden, and

vi. the unilateral ceasefire Ganaa Islamiya declared against the Egyptian government.

[127] Mr. Mahjoub argues that if the Service is aware of exculpatory information or information harmful to its case, it must disclose this information to the designated judge in the *ex parte* warrant process as part of its duty of full, fair and frank disclosure. Mr. Mahjoub alleges that the Service was aware of such information and failed to disclose it. He argues that if it had disclosed this information, there would be no foundation left to the allegations against him.

[128] Moreover, Mr. Mahjoub alleges that the Service misled the designated judge in its affidavits. Mr. Mahjoub further submits that it does not matter whether the affiant intended to mislead the court. In support of this latter proposition he relies on *Morelli*, at paragraph 59.

[129] Even if Mr. Mahjoub were to establish that there were material omissions, inaccuracies, or misleading statements in the affidavits before the designated judge, this may not be sufficient to find the warrants unlawful. The presumption of validity is so strong that even in the *Criminal Code* warrants context, the accused person must prove that the warrant could not have issued but for the omission, inaccuracy or misleading statement. As the Supreme Court maintains in *Garofoli* at page 1452:

> The reviewing judge does not substitute his or her view for that of the authorizing judge. If, based on the record which was before the authorizing judge as amplified on the review, the reviewing judge concludes that the authorizing judge could have granted the authorization, then he or she should not interfere. In this process, the existence of fraud, non-disclosure, misleading evidence and new evidence are all relevant, but, rather than being a prerequisite to review, their sole impact is to determine whether there continues

> to be any basis for the decision of the authorizing judge. [Emphasis added]

[130] Even *Morelli* confirms this approach. At paragraph 60, Justice Fish states:

> The facts originally omitted must be considered on a review of the sufficiency of the warrant application. In *Araujo*, the Court held that where the police make good faith errors in the drafting of an ITO, the warrant authorization should be reviewed in light of amplification evidence adduced at the voir dire to correct those mistakes. Likewise, where, as in this case, the police fail to discharge their duty to fully and frankly disclose material facts, evidence adduced at the voir dire should be used to fill the gaps in the original ITO.

[131] Having reviewed the applicable legal principles, I will now turn to consider the affidavits and warrants at issue. Since these materials, with the exception of the public summaries delivered to Mr. Mahjoub, are for the most part classified, my reasons on the issue are found in "Section C" of the Confidential Annex. I insert below a summary of my findings on this issue from the Confidential Annex.

[132] I am satisfied that all of the alleged omissions and misrepresentations in the affidavits postulated by Mr. Mahjoub have no merit, except for one instance that was dealt with more fully *in camera* by the Special Advocates and two instances that had no bearing on the decision. In some instances, the Service did not or could not have known the allegedly "omitted" information. In other instances, the Service provided the allegedly "omitted" information to the issuing judge. In addition, with respect to Professor Wark and Professor Gerges's expert opinions and criticisms of the SIR, they are the product of many additional years of knowledge and of these adversarial

proceedings. The Service could not have been expected to have the same knowledge more than a decade earlier as that provided to the Court by Professors Wark and Gerges.

[133] By reason of certain omissions raised by the Special Advocates, comprehensively dealt with in "Section C" of the Confidential Annex, and the Service's failure to distinguish between facts and analysis on certain points in the affidavit, I found that the Service breached its duty of full, fair and frank disclosure. Nevertheless, I also found that the breach did not invalidate the warrant. I was satisfied with the omitted information supplied and the misleading information corrected in the affidavit (*Morelli* at paragraph 60), the warrant could have issued (*Garofoli* at page 1452). Consequently, there is no need for me to interfere. There would still have been sufficient evidence to satisfy the designated judge that there were reasonable grounds to believe that a warrant was required to investigate the threat.

(c) *The absence of any indication that the warrants complied with the requirements of the* CSIS Act*, namely sections 21(1) and 21(2)*(a) *to* (g)*?*

[134] It is useful to consider the applicable standard of review of a designated judge's decision to issue a section 21 warrant. As discussed above, if the issue concerns the inclusion of misleading information or the failure to include exculpatory information in the affidavits, then the test is whether the warrants could issue notwithstanding the deficiencies.

[135] The standard to be applied to a review of a designated judge's discretionary decision on the merits of the section 21 application is necessarily different. The

circumstances of the review are quite particular. The review concerns the discretionary decision of a colleague on the same court and not an inferior administrative tribunal. The legislative scheme provides little assistance in that no provision is made for such a review by way of an appeal or judicial review application. The Supreme Court provides limited guidance, namely that a reviewing court must take care not to substitute its discretion for the discretion of the designated judge (*Garofoli* at page 1452).

[136] In my view, in conducting such reviews, deference is owed to the designated judge who issued the warrant. A reviewing court may only interfere with such a discretionary decision in the presence of a palpable and overriding error (*Housen v. Nikolaisen*, 2002 SCC 33 at paragraph 36; *Dunsmuir v. New Brunswick*, 2008 SCC 9 at paragraph 51, and paragraph 161 of the concurring reasons). This is the standard that I will apply to the issues raised by Mr. Mahjoub in his challenge to the warrants.

[137] Although Mr. Mahjoub has challenged the lawfulness of the warrants pursuant to paragraph 21(1) of the Act, he has not expressly raised any issue concerning the Service's alleged failure to comply with this provision. To the extent that Mr. Mahjoub alleged that the Service failed to establish that a warrant was required to investigate the threat posed by Mr. Mahjoub, I shall address this issue in the context of what the Service presented to the designated judge in accordance with paragraph 21(2)(*a*) below.

[138] Mr. Mahjoub alleges that the Court erred in issuing the warrants because the information relied upon in the affidavits in support of these warrants cannot be relied upon.

[139] Mr. Mahjoub's general submission is that the warrants are not and cannot be compliant with the requirements of the *CSIS Act* because the affidavits upon which the designated judge issued the warrants were based on unsourced and therefore unreliable information, with conclusory statements, and containing no indicia of reliability. The only exception to this, raised by Mr. Mahjoub, is the Service's interviews with him, which he argues must be excised due to the Service's failure to inform him of his right to counsel. In support of his argument, Mr. Mahjoub relies on *R. v. Hosie* (1996), 107 C.C.C. (3d) 385 at page 391 (Ont. C.A.). In that case, the Ontario Court of Appeal discusses reliability in dealing with unknown sources in a warrant affidavit requiring courts to consider the following factors:

(a) Was the information predicting the commission of a criminal offence compelling?

(b) Where that information was based on a "tip" originating from a source outside the police, was that source credible?

(c) Was the information corroborated by police investigation prior to making the decision to conduct the search?

[140] Concerning Mr. Mahjoub's argument on the inherent unreliability of the "unsourced" information, this issue is addressed in of the *Foreign Agency Evidence*

Decision. In that decision, I found that the "unsourced" foreign agency evidence was not categorically unreliable, and that the Court in this proceeding could consider it. By analogy, the Service and the designated judge in the warrant proceedings were also entitled to consider and rely on it.

[141] I now turn to Mr. Mahjoub's argument concerning the absence of any indicia of reliability in the information supporting the warrants.

[142] In *United States of America v. Ferras*, 2006 SCC 33, at paragraphs 3 and 11, individuals subject to extradition orders made similar arguments that the statutory scheme allowed them to be extradited on inherently unreliable evidence, and that there were inadequate safeguards built into the regime. In the extradition context, the requesting state is only required to provide a certificate which is a "threshold indicator of reliability," and the evidence relied upon by the requesting state, even if considered unreliable and inadmissible in Canada, is admissible at the extradition hearing (at paragraph 31). At paragraph 33, the Supreme Court explains that the principles of fundamental justice with respect to the reliability of evidence are contextual:

> The absence of particular indicia of reliability or availability of evidence in itself does not violate the principles of fundamental justice applicable to extradition hearings. No particular form or quality of evidence is required for extradition, which has historically proceeded flexibly and in a spirit of respect and comity for extradition partners. It is thus difficult to contend that the provisions of the Act for the admissibility of evidence, in and of themselves, violate the fundamental norms of justice applicable to extradition.

[143] The Supreme Court indicates at paragraph 34 that "[w]hat fundamental justice does require is that the person sought for extradition be accorded an independent and impartial judicial determination on the facts and evidence on the ultimate question of whether there is sufficient evidence to establish the case for extradition."

[144] In my view, there is an analogy to be drawn between extradition and the *CSIS Act* warrant process. In both proceedings, the named person is not subjected to a Canadian criminal investigation. The nature of information is similar, the exchange of information with foreign agencies with limited information relating to its provenance. Finally, in both, judicial proceedings have yet to initiate.

[145] Further, unlike the extradition context which could subject the individual to removal from Canada, the warrant process only engages the named person's privacy interest. Therefore, the consequential impact on the named person which could potentially flow from the processes is likely to be less severe in the warrant situation.

[146] In a warrant application, the issuing judge is well aware of the particular circumstances under which the application is made. As with any *ex parte* application, the judge is sensitive to the fact that an interested party is absent and that his or her interests are not being represented. In such circumstances, a designated judge will scrutinize the evidence and pose questions to the affiant on the evidence or on any issue that requires clarification.

[147] I am satisfied, as in extradition cases, that the absence of particular indicia of reliability or availability of evidence in itself does not violate the principles of fundamental justice. It is open to the judge to question the reliability of any information adduced in support of a warrant. In this instance, the judge issuing the warrant was entitled to evaluate the information in the affidavit notwithstanding the lack of any particular indicia of reliability. This is particularly appropriate in the context of determining whether a warrant is needed for further investigation.

[148] In "Section D" of the Confidential Annex, I review the content of the information contained in the affidavits adduced in support of a particular warrant at issue. I provide therein my analysis of the issue raised by Mr. Mahjoub concerning the reliability of the information. I am satisfied that disclosure of that discussion would be injurious to national security or to the safety of persons. I insert below a summary of my findings on this issue.

[149] I cannot substitute my discretion for that of the designated judge who issued the warrant, particularly on the determinative question of whether there are reasonable grounds to believe a warrant is necessary for a Service investigation. The Service provided detailed information including sources and corroboration as indicia of reliability on the existence and seriousness of the threat to the security of Canada. In these circumstances, it was reasonably open to the designated judge to find that the affidavits satisfied paragraph 21(2)(*a*).

[150] In the result, I reject Mr. Mahjoub's argument that the warrant should not have issued on the basis that the evidence relied upon by the Service in support of the warrant were insufficiently reliable.

[151] Mr. Mahjoub argues that interviews between him and Service personnel are inadmissible because the Service personnel did not inform him of his right to counsel. This submission is without merit. Section 10(*b*) of the *Charter* is a right that is engaged only when an individual is arrested or detained.

[152] The test for detention is found in *R. v. Therens*, [1985] 1 S.C.R. 613, whether a reasonable person in Mr. Mahjoub's position would have believed him or herself to be physically or legally compelled to do what an agent of the state asked. There must be:

(a) An authoritative "demand or direction", rather than a mere request, in response to which

(b) "the person concerned submits or acquiesces in the deprivation of liberty and reasonably believes the choice to do otherwise does not exist."

When a foreign national was required to undergo a second examination for his immigration screening, the Supreme Court found that he was not detained in the sense intended by section 10(*b*) of the *Charter*, and the principles of fundamental justice did not require him to be provided with counsel under section 7 of the *Charter* (*Dehghani v. Canada (Minister of Employment and Immigration*), [1993] 1 S.C.R. 1053). Further, suspects stopped by the police for interviews are not necessarily "detained" in the sense of section 10(*b*) (*R. v. Mann*, 2004 SCC 52 [*Mann*]).

[153] Based on the above jurisprudence, I find that when Mr. Mahjoub voluntarily agreed to answer questions of Service personnel, he was not "detained" in any legal sense. Moreover, there is evidence before the Court that, at several reprises, the Service personnel interviewing him asked him whether he wished to consult counsel, and he declined that invitation (see the October 5, 1998 and March 31, 1999 interviews). There was no reason for the designated judge to exclude the evidence of Mr. Mahjoub's interviews with Service personnel, and there is no reason for the Court to consider their inclusion in the affidavit to be inappropriate now.

[154] Mr. Mahjoub contends that the affidavits do not demonstrate reasonable grounds to believe that warrants are necessary to investigate the threat to the security of Canada allegedly posed by Mr. Mahjoub, and that there is no indication in the warrants that the matter is urgent and other investigative procedures have failed or are unlikely to succeed.

[155] The Special Advocates have made more particularized submissions in support of Mr. Mahjoub's argument. In my view, disclosure of these particulars would be injurious to national security or to the safety of persons. My analysis of the affidavits' compliance with paragraph 21(2)(*b*) may therefore be found in "Section E" of the Confidential Annex. I insert below a summary of my findings on this issue from the Confidential Annex.

[156] Concerning paragraph 21(2)(*b*) in particular, I am satisfied that the designated judge committed no palpable and overriding error in finding that the Service's justification for the necessity of the warrant against Mr. Mahjoub was sufficient.

[157] Paragraphs 21(2)(*c*) to (*g*) may be dealt with together. Mr. Mahjoub submits that there is no indication of the type of communication that the Service proposes to intercept, or the identity of the person or persons whose communications shall be intercepted, or the classes of person at whom the warrant is directed, or the place and period for which the warrant is requested.

[158] Mr. Mahjoub alleges that:

a. There is no indication of the type of communication that the Service proposes to intercept, as required by paragraph 21(2)(*c*);

b. The person or persons whose communications the Service proposes to intercept are not identified, as required by paragraph 21(2)(*d*);

c. There is no indication of the classes of persons at whom the Service directs these warrants, as required by paragraph 21(2)(*e*);

d. There is no general description of the place where the Service proposes to execute the warrant, as required by paragraph 21(2)(*f*), and

e. There is no indication of the period for which the Service requests the warrant, as required by paragraph 21(2)(*g*).

[159] Summaries of the content of the affidavits and warrants were prepared on a collaborative basis by the Special Advocates and the Ministers' Counsel and released to Mr. Mahjoub by Order dated October 5, 2010. While these summaries provide significant detail pertaining to the content of the affidavits and warrants, further disclosure of particulars relating to the requirements of paragraphs 21(2)(*c*) to (*g*) would be injurious to national security or to the safety of any person. These details are found in "Section F" of the Confidential Annex. I insert below a summary of my findings on this issue from the Confidential Annex.

[160] Mr. Mahjoub's allegations concerning paragraphs 21(2)(*c*) to (*g*) are largely speculative. The Service provided details addressing the requirements of paragraphs 21(2)(*c*) to (*g*). It was reasonably open to the designated judge to find that the affidavits satisfied these provisions.

(d) *The warrants' authorization of solicitor-client interceptions, which constitutes unreasonable search and seizure?*

[161] Lastly, concerning the issue of the validity of the warrants, Mr. Mahjoub submits that if the section 21 warrants authorized the Service to intercept his solicitor-client privileged communications, they are unlawful because they authorize unreasonable search and seizure violating section 8 of the *Charter*.

[162] While *Blood Tribe* confirms that solicitor-client privilege is a substantive right that is an integral component of the right to a fair trial under section 7 of the *Charter* that may only be infringed when absolutely necessary, it does not deal with a situation involving national

security. The Federal Court of Appeal in *Atwal* maintains that it is permissible for section 21 warrants issued under the *CSIS Act* to infringe solicitor-client privilege when there are adequate safeguards provided in the warrant to prevent the dissemination of privileged information.

[163] If specifically authorized and with restrictions on the use of solicitor-client intercepts to minimally impair solicitor-client privilege as there were in *Atwal*, in my view, section 21 warrants can permit the Service to intercept all communications from a target, including the incidental interception of solicitor-client privileged information.

[164] Disclosure of the details relating to warrant powers authorized in specific warrants and the conditions imposed on the authorizations would, in my opinion, be injurious to national security or to the safety of persons. Consequently, consideration of these details and my analysis on the issue may be found in "Section G" of the Confidential Annex. I insert below a summary of my findings on this issue from the Confidential Annex.

[165] I am satisfied that the warrants issued prior to Mr. Mahjoub's arrest, which authorize the interception of communications and therefore the incidental interception of solicitor-client communications, provide adequate safeguards to prevent the dissemination of privileged information. Consequently, in accord with the jurisprudence of the Court of Appeal in *Atwal*, the warrants are permissible and do not violate section 8 of the *Charter*.

[166] In addition, Mr. Mahjoub argues that there was an absence of sufficient safeguards within the Service to ensure that only threat-related intercepts (including solicitor-client intercepts) were collected and stored, and that these intercepts would not be passed on. He argues that failure to do so would amount to an invalidation of the warrants. In support of his argument, he relies on *Lavallee*. In that case, the Supreme Court examines legislative safeguards of solicitor-client privilege in the context of criminal investigations in which the police are searching documents in the possession of a lawyer. Mr. Mahjoub maintains the principles therein are applicable to this case, particularly with regards to the Service's policy of destroying the intercepts.

[167] In my view this argument has no merit. There is no connection with the Court's authorization of warrant powers and the Service's internal procedures for the safeguarding of information. The alleged deficiencies in the Service's internal safeguard were raised and dealt with in the context of the *Abuse of Process Decision* at paragraph 218.

[168] To conclude, in my view, *Atwal* resolves the issue of whether warrants issued prior to Mr. Mahjoub's detention that authorize solicitor-client intercepts are lawful. In *Atwal*, the Court of Appeal held that the restrictions in the warrant placed on the dissemination of solicitor-client privileged information gathered under its authority rendered the warrant constitutionally compliant. Such conditions, or internal Service policies reflecting the conditions in the *Atwal* warrant, would be constitutionally compliant (at pages 10, 17). Upon verifying the warrants at issue, I find them to be compliant with the *Charter*.

[169] Regarding the warrants that issued subsequent to Mr. Mahjoub's detention, these warrants are not governed by the principles set out in *Atwal* but rather, by those set out in *Solosky* for the reasons set out at paragraphs 82 and 86 above. Disclosure of any details pertaining to such warrants would be injurious to national security or to the safety of any person. This issue will be further discussed at "Section G-1" of the Confidential Annex. A summary of my findings is included below.

[170] Since the warrants authorized the incidental interception of solicitor-client privileged communications without the appropriate restrictions required to protect Mr. Mahjoub's section 7 and section 8 *Charter* rights as defined by *Solosky*, certain provisions in the warrant or warrants issued after Mr. Mahjoub's arrest are unlawful. The appropriate remedy would be to exclude any evidence resulting from those warrant provisions. However, no such evidence was adduced in these proceedings, and therefore no remedy beyond a declaration that Mr. Mahjoub's section 7 and section 8 rights have been violated is required in the circumstances. There is therefore no need for me to decide to what extent the inadequate protection of Mr. Mahjoub's *Charter* rights impacts upon the validity of these warrants.

4. *Did CSIS engage in searches and seizures that were not authorized by the section 21 warrants and not otherwise authorized by law?*

[171] The summaries of the section 21 warrants do not contain the particulars of what they did and did not authorize. Mr. Mahjoub therefore argues in the alternative that the Service and other government agencies conducted searches and seizures that were not authorized by the warrants and were not otherwise lawful. He again raises the intercepts

of solicitor-client communications. Also challenged are intercepts of the communications of individuals who do not appear to be named in the warrants, such as Mona El Fouli and Essam Marzouk, the telephone toll records obtained from his service provider and the physical seizure of his address book and the investment letter from Mubarak Al Duri.

[172] There is no dispute that solicitor-client privileged intercepts obtained without a warrant are inadmissible in evidence against Mr. Mahjoub. In this case, the Ministers are not relying on any solicitor-client privileged information, so none of it is before the Court for the purposes of the reasonableness determination.

[173] Any argument relating to prejudice to Mr. Mahjoub's case flowing from solicitor-client intercepts have been dealt with in the *Abuse of Process Decision*.

[174] In addition, Mr. Mahjoub argues that the Service intercepted the communications of Mona El Fouli, Hani El Fouli and Essam Marzouk despite the absence of their names in the warrants and the fact that they were "known" to the Service. He therefore contends that the warrants are invalid on the grounds set out in *R. v. Chesson*, [1988] 2 S.C.R .148, with respect to the appellant Vanweenan. The Vanweenan ground for invalidity found in criminal proceedings relies on paragraphs 178.12(1)(*e*) and 178.12(1)(*c*) of the *Criminal Code* that require all "known" persons as specifically defined in the *Code* to be named in the warrant (*Garofoli* at page 1445). The *CSIS Act* has no analogous provisions. Subsection 21(2)(*d*) only requires the Service to indicate which individuals it proposes to

intercept, if known, and subsection 21(4)(*b*) only requires the warrant to indicate which individuals are to be intercepted, if known.

[175] Nevertheless, the Court should not permit the Service to obtain a warrant on one individual in order to intercept the communications of another who is known to the Service. The Service should be required to seek a warrant for any individual on or from whom it seeks information in the investigation at issue. Thus, in spite of the differences between the *Criminal Code* and the *CSIS Act*, I shall examine whether the interception of Mona El Fouli, Hani El Fouli and Essam Marzouk was authorized by the warrants.

[176] As the disclosure of whom precisely the warrants named and during what periods would, in my opinion, be injurious to national security and the safety of persons, my analysis of this issue is to be found in "Section H" of the Confidential Annex. I insert below a summary of my findings on this issue from the Confidential Annex.

[177] The scope of the warrants extended to those individuals whose communications the Service intercepted. Upon review of the classified materials, I am satisfied that no communications of the third persons identified by Mr. Mahjoub were intercepted without warrant authorization.

[178] In my view, the particulars of what techniques were authorized by each warrant also cannot be disclosed without injury to national security or the safety of persons. My reasons disposing of Mr. Mahjoub's allegations that the interception of the telephone toll

records and the seizure of the letter from Mr. Al Duri were not authorized may be found in "Section I" of the Confidential Annex. I insert below a summary of my findings on this issue from the Confidential Annex.

[179] The Service's search of Mr. Mahjoub's briefcase and seizure of the August 1998 letter from Mr. Al Duri was authorized by warrant as the Ministers argue, relying on the testimony of Mr. Michel Guay (13 October 2010, p.44). Upon review of the classified materials, I am satisfied that the seizure of both the toll records and letter from Mr. Al Duri to Mr. Mahjoub were authorized by warrant.

[180] The police seized Mr. Mahjoub's address book and "pocket litter" at the time Mr. Mahjoub was being arrested on June 26, 2000. It is a classic example of "search incidental to arrest," one of the most recognized exceptions to the requirement of a warrant in the common law. *R. v. Stillman*, [1997] 1 S.C.R. 607 [*Stillman*], defines the conditions of this kind of search (at paragraph 27). Of course, the arrest must first be lawful and not arbitrary. I found at paragraph 173 of the *Constitutional Decision* that section 81 of the *IRPA* does not authorize arbitrary detention. I am therefore satisfied that because a security certificate was duly signed by the Ministers naming Mr. Mahjoub, his arrest pursuant to that certificate was lawful and not arbitrary. Second, the search must be "incidental" to the arrest, particularly for the protection of the arresting officers to prevent the destruction of evidence or to discover evidence (*Mann* at paragraph 37; *R. v. Caslake*, [1998] 1 S.C.R. 51 at paragraph 15). Searching Mr. Mahjoub's pockets is included in this category of search. Third, the search must be carried out in a reasonable manner. Mr.

Mahjoub has not alleged that the arresting officers conducted the search in an unreasonable or abusive manner.

[181] Since the Ministers considered Mr. Mahjoub to be a significant security threat, the police were justified in searching Mr. Mahjoub's person to ensure their own safety (*Stillman* at paragraph 48). Searching Mr. Mahjoub's pockets was also a reasonable measure to prevent him from disposing of the evidence contained therein (*ibid.*). The results of that search can be used in evidence against Mr. Mahjoub.

[182] The admissibility of the telephone toll record and address book evidence was challenged by Mr. Mahjoub during the reasonableness proceeding in open court. The Court heard extensive arguments from the parties on October 13 and 15, 2010, and subsequently ruled on the admissibility of the evidence on the basis of those arguments. I rendered my decision from the bench on October 22, 2010, ruling that the evidence was admissible. In my reasons, I held that Mr. Mahjoub had failed to establish any evidentiary foundation for his objection. I noted that the evidence in question had been disclosed to Mr. Mahjoub well in advance of the reasonableness hearing and in sufficient time to request further information on how the evidence was obtained. I also noted that Mr. Mahjoub had made no request for further disclosure of the underlying authorities relating to the searches and seizures of the telephone records at issue.

[183] The Ministers argue that Mr. Mahjoub has implicitly waived his objections to the searches and seizures of the telephone toll records and physical evidence because of the

extensive passage of time, citing *Almrei (Re)*, 2009 FC 1263 at paragraph 19. Mr. Mahjoub contends that Ms. Joncas attempted to object to the evidence when introduced, but the Court ruled in favour of leaving the issue of its admissibility until later. Since in my above reasons, I have determined that the search and seizure of toll records and physical evidence at issue was lawful, there is no need to address this issue.

5. *If evidence used in this proceeding was unlawfully obtained for any of the above reasons, should it nevertheless be admissible pursuant to subsection 24(2) of the* Charter*?*

[184] I have found one or more of the warrant powers to be unlawful because they authorized the incidental interception of solicitor-client communications without reasonable and probable grounds after Mr. Mahjoub's detention. However, no evidence was adduced in these proceedings as a result of any of those warrants that has not already been excluded as demonstrated at paragraph 4 above: all of the remaining evidence pre-dates Mr. Mahjoub's arrest. There is therefore no need for me to conduct an analysis pursuant to subsection 24(2) of the *Charter* to determine whether the evidence obtained from the warrants should nevertheless be admissible because it does not bring the administration of justice into disrepute.

Conclusion

[185] To conclude, the impugned provisions of the *CSIS Act* are not unconstitutional on the grounds alleged by Mr. Mahjoub, the warrants obtained by the Service pursuant to section 21 of the *CSIS Ac*t during its investigation of Mr. Mahjoub prior to his arrest are lawful, and although certain powers in the warrant or warrants obtained by the Service

pursuant to section 21 of the *CSIS Act* after Mr. Mahjoub's arrest were unlawful, the evidence that Mr. Mahjoub challenges was obtained lawfully.

[186] "Threat to the security of Canada" defined in section 2 and the investigative procedures authorized by section 12 of the *CSIS Act* are neither vague nor overbroad. Mr. Mahjoub's *Charter* rights are not engaged by section 6 even in theory. Section 17 strikes the required balance between individual rights to privacy and public interest concerns and is not unconstitutional because it permits information-sharing with foreign agencies. The warrants provisions, sections 21 to 24, are not unconstitutional simply because they permit a warrant to authorize the interception of solicitor-client communications. As long as conditions are in place to prevent dissemination of any privileged information, *Atwal* indicates that section 21 warrants may authorize the interception of solicitor-client communications in the circumstances of a prospective investigation into a threat to the security of Canada prior to arrest or the commencement of judicial proceedings.

[187] Mr. Mahjoub's challenge to the validity of the warrants does not constitute a collateral attack on the issuing judges' decisions pursuant to section 21 because it is a motion to exclude evidence obtained under the authority of the warrants pursuant to sections 8 and 24(2) of the *Charter*. The only way to establish a section 8 violation in the collection of evidence authorized by a warrant is to challenge that warrant. The evidence may not, however, be excluded on the basis of the unconstitutionality of the previous *IRPA* regime, nor may it be excluded because the affidavits and warrants are not disclosed in their original form to Mr. Mahjoub and his counsel.

[188] Moreover, the warrants with the exception of certain warrant powers noted above, are lawful. I have come to the conclusion that the affidavits supporting the Service's application for warrants were potentially misleading and lacked some material particulars. Nevertheless, while the Service breached its duty to provide the issuing judges with full, fair and frank disclosure, I am satisfied that the warrants could have issued in any event. Further, it was open to the issuing judge to find that the affidavits complied with paragraphs 21(1)(*a*) to (*g*) of the *CSIS Act*, and there is no error that requires my interference with their decisions. Lastly, the warrants themselves comply with subsection 21(4) of the *CSIS Act*.

[189] Finally, the evidence that Mr. Mahjoub seeks to exclude in this application was collected lawfully and did not violate section 8 of the *Charter*. I find that the collection of the items listed at paragraph 4 of these Reasons was duly authorized by warrants as the Ministers claim. The specifics of these authorizations may be found in the "Conclusion" section of the Confidential Annex since disclosing these would be injurious to national security or to the safety of any person. The search of Mr. Mahjoub's home to obtain the letter from Mr. Al Duri and the search of Mr. Mahjoub's person upon his arrest from which pocket litter as obtained were also lawful.

[190] For the above reasons, I will dismiss Mr. Mahjoub's application.

ORDER

THIS COURT ORDERS that the motion is dismissed.

"Edmond P. Blanchard"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET: DES-7-08

STYLE OF CAUSE: **IN THE MATTER OF A CERTIFICATE SIGNED PURUSANT TO SECTION 77(1) OF THE *IMMIGRATION AND REFUGEE PROTECTION ACT (IRPA)*;**

AND IN THE MATTER OF THE REFERRAL OF A CERTIFICATE TO THE FEDERAL COURT PURSUANT TO SECTION 77(1) OF THE *IRPA*

AND IN THE MATTER OF MOHAMED ZEKI MAHJOUB

PLACE OF PUBLIC HEARING: TORONTO, ONTARIO / OTTAWA, ONTARIO

DATES OF PUBLIC HEARING: OCTOBER 12, 13, 15, 18, 19, 20, 21, 22, 25, 26, 27, 2010
NOVEMBER 1, 2, 23, 24, 25, 29, 30, 2010
DECEMBER 1, 6, 7, 8, 14, 15, 2010
JANUARY 10, 11, 12, 17, 19, 20, 21, 2011
JUNE 2, 3, 9, 13, 14, 15, 17, 20, 21, 27, 28, 29, 2011
JULY 4, 5, 6, 7, 8, 11, 12, 13, 14, 2011
JULY 24, 25, 26, 2012
AUGUST 1, 8, 2012
SEPTEMBER 6, 9, 10, 11, 12, 2012
NOVEMBER 26, 27, 28, 29, 30, 2012
DECEMBER 3, 4, 6, 7, 10, 2012

REASONS FOR ORDER AND ORDER: BLANCHARD J.

DATED: OCTOBER 25, 2013

APPEARANCES:

Mr. Donald MacIntosh Mr. David Tyndale Mr. Bernard Assan Mr. Peter Southey Ms. Marianne Zoric Ms. Mahan Keramati Mr. Christopher Ezrin Ms. Balqees Mihirig Ms. Judy Michaely Ms. Rhonda Marquis Mr. James Mathieson Mr. Marcel Larouche Mr. Toby Hoffmann Ms. Proja Filipovich Mr. Philippe Lacasse Ms. Erin Bobkin Ms. Dominique Castagne	FOR THE APPLICANTS MINISTER OF CITIZENSHIPAND IMMIGRATION AND MINISTER OF PUBLIC SAFETY
Ms. Johanne Doyon Mr. Paul Slansky Mr. Yavar Hameed Mr. David Kolinsky Mr. Khalid Elgazzar Ms. Lucie Joncas	FOR THE RESPONDENT MR. MOHAMED ZEKI MAHJOUB
Mr. Gordon Cameron Mr. Anil Kapoor	SPECIAL ADVOCATES

SOLICITORS OF RECORD:

William F. Pentney Deputy Attorney General of Canada Ottawa, Ontario	FOR THE APPLICANTS

Johanne Doyon Doyon & Associés Montreal, Quebec	FOR THE RESPONDENT
Paul B. Slansky Slansky Law Professional Corp. Toronto, Ontario	
Yavar Hameed Hameed & Farrokhzad Ottawa, Ontario	
David Kolinsky Barrister & Solicitor Edmonton, Alberta	
Gordon Cameron Ottawa, Ontario	SPECIAL ADVOCATE
Anil Kapoor Toronto, Ontario	SPECIAL ADVOCATE