Federal Court  Cour fédérale

Date: 20131122

Docket: CSIS-30-08

Citation: 2013 FC 1275

Ottawa, Ontario, November 22, 2013,

PRESENT: THE HONOURABLE MR. JUSTICE MOSLEY

BETWEEN:

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

AND IN THE MATTER OF [ ]

REDACTED AMENDED FURTHER REASONS FOR ORDER

MOSLEY J.

INTRODUCTION:

[1] On May 4, 2009 the Court issued Reasons for the issuance of a warrant to intercept foreign telecommunications and [ ] from within Canada. An amended and redacted public version of those reasons was released on October 5, 2009. The warrant was issued initially on January 26, 2009 for a period of three months and was reissued for a further 9 months on April 6,

2009. When first authorized, the warrant marked a departure from the position previously taken by the Court that it lacked jurisdiction to authorize the collection of security intelligence information concerning a threat to the security of Canada by the Service from countries other than Canada. In my private and public reasons I explained why I considered it appropriate to authorize the collection of foreign telecommunications and [ ] so long as the interception of the telecommunications and seizures of the information took place from and within Canada.

[2] In arriving at that decision, I was persuaded by the applicant's legal argument as to how the proposed method of interception was relevant to the jurisdiction of this Court and by a description of the facts concerning the methods of interception and seizure of the information, which differed from that put before my colleague, Justice Edmond Blanchard, on a prior application. More precisely, the applicant argued that this Court had jurisdiction to issue warrants to ensure a measure of judicial control over activities by government officials in Canada in relation to an investigation that extends beyond Canadian borders. Counsel advanced the argument that this Court had such jurisdiction because the acts the Court was being asked to authorize would all take place in Canada.

[3] Since my May 2009 Reasons were issued, a number of similar warrants have been issued on fresh or renewed applications in relation to other targets of investigation under sections 12 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 ("the CSIS Act"). In these Reasons, I will refer to these warrants as "CSIS-30-08 warrants" or "30-08".

[4] These Further Reasons for Order respond to recent developments and are intended to clarify the scope and limits of the Reasons issued in 2009. This has become necessary, in my view, as a result of additional information that has been provided to the Court following publication of the 2012-13 Annual Report of the Commissioner of the Communications Security Establishment Canada (CSEC), the Honourable Robert Décary, QC. These Further Reasons address issues that have arisen with respect to whether the duty of full disclosure owed by the Canadian Security Intelligence Service ("CSIS or the Service") to the Court was respected and with regard to foreign collection practices undertaken by the Service and CSEC in connection with the issuance of the 30-08 warrants.

[5] Before addressing these issues, I think it important to lay out my understanding of the background to these events for the record.

BACKGROUND:

[6] CSIS has long taken the position that it is not barred by its statute from engaging in security intelligence collection activities outside of Canada. This view is supported by the absence of an express territorial limitation in s 12 of the Act, by statements made in the *Report of the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police 1981* (McDonald Commission) which led to the creation of the Service, and by statements in Parliament during the debates prior to enactment of the enabling statute. The Service has engaged in certain investigative activities in foreign countries by, among other things, [

] entering into sharing agreements with foreign agencies.

[7] The question which remained in doubt, however, was whether the conduct of intrusive activities abroad that in Canada required lawful authority, such as a warrant or express enabling legislation, would contravene the *Canadian Charter of Rights and Freedoms*, enacted as Schedule B to the *Canada Act*, 1982, (U.K.) 1982 c. 11 and the *Criminal Code*, R.S.C. 1985, c C-46. In the absence of express legislative authority, or a warrant, it was considered by the Service and its legal advisors that CSIS officers would be exposed to potential liability in Canada as well as in the foreign jurisdiction. While this could have been addressed by Parliament, no attempt was made to amend the legislation, most likely due to concerns about the controversy that opening the Act to insert such an amendment would engender.

[8] The Service did not attempt to seek the authorization of a warrant to conduct intrusive activities abroad until 2005. In that year, the Service applied for a warrant, in application CSIS 18-05, that if issued would have authorized the interception of the communications of a Canadian citizen who was temporarily resident outside Canada. The requested warrant would also have authorized the Service to obtain, in relation to the target, [

].

[9] A preliminary issue arose as to whether the questions of law raised by the application could be dealt with in a public hearing. An *amicus curiae*, Mr. Ron Atkey QC, was appointed to assist the

Court in determining that issue. Following oral and written submissions, Justice Simon Noël concluded that the application should be dealt with in private. A public version of his Reasons for Order and Order was released in 2008: *Re Canadian Security Intelligence Services Act* 2008 FC 300, [2008] F.C.R. 477. For operational reasons, a notice of discontinuance of the application was filed on August 23, 2006 without a determination of the merits or other legal issues.

[10] The questions were then raised again in an application (CSIS 10-07) brought before Justice Edmond Blanchard in April, 2007. In that application, CSIS sought the authority of warrants in respect of investigative activities against 10 subjects in Canada and other countries. On the strength of the evidence of a CSIS affiant, Justice Blanchard was satisfied that the requirements of paragraphs 21 (2) (a) and (b) of the *CSIS Act* had been met for the issuance of warrants for execution in Canada. However, he was not prepared to authorize investigative activities by the service outside Canada, as requested, without further consideration. Mr. Ron Atkey was again appointed to serve as *amicus curiae*. Justice Blanchard requested that the Service and the *amicus* file written submissions to address first, whether the Service has a mandate to undertake threat related investigations outside Canada and second, whether the Federal Court had jurisdiction to issue the requested warrant.

[11] In the application before Justice Blanchard, the Service sought a warrant to intercept any telecommunication destined to or originating from the subjects of investigation including such communications abroad; to obtain information or records relating to the targets [

] It was requested that the warrant provide that it may be executed, in addition to locations in Canada, at any place outside of Canada under the control of the government of Canada or of a foreign government. [

].

[12] In addition to the evidence of the CSIS affiant required to establish the statutory prerequisites to the issuance of a warrant, counsel for the applicant filed the affidavit evidence of James D. Abbott, CSEC's then Acting Director of Signals Intelligence ("SIGINT") Requirements.

[13] CSEC's mandate is set out in the *National Defence Act*, R.S.C. 1985, c. N-5, as amended by the *Anti-terrorism Act*, S.C. 2001, c. 41. Under paragraph 273.64(1) (a) of this statute, the agency is authorized to acquire and use information from the global information infrastructure (i.e., communications systems, information technology systems and networks) for the purpose of providing foreign intelligence to the government of Canada.

[14] Prior to the 2001 legislation, it was unlawful for CSEC to intercept the communications of a foreign target that either originated or terminated in Canada. Under the then prevailing regimen, CSEC could only target communications that originated and terminated in foreign jurisdictions, and which involved foreign intelligence. The 2001 legislation empowered the Minister of National Defence to authorize CSEC to target foreign entities physically located outside the country that may engage in communications to or from Canada, for the sole purpose of obtaining foreign intelligence.

A major factor prompting the legislation was CSEC's need for lawful authority to operate effectively without transgressing the *Criminal Code* prohibition against intercepting "private communications", as will be discussed further below. The legislation enabled CSEC to intercept communications to or from Canada for the purpose of obtaining foreign intelligence subject to ministerial authorization and contingent on specific provisos set out in s 273.65 (2):

> a) the interception is directed at foreign entities outside of Canada;
> b) the information could not reasonably be obtained by other means;
> c) the expected foreign intelligence value of the information justifies its collection; and
> d) satisfactory measures are in place to protect the privacy of Canadians to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

[15] CSEC is expressly prohibited under paragraph 273.64(2) (a) of the *National Defence Act* from directing these activities at Canadian citizens and permanent residents ("Canadian persons") wherever located or at any person in Canada regardless of nationality.

[16] The limitations respecting Canadian persons and any persons in Canada do not apply to technical and operational assistance which CSEC may provide to federal law enforcement and security agencies in the performance of their lawful duties pursuant to paragraph 273.64(1) (c) of the *National Defence Act*. Subsection 273.64(3) of this statute provides that such assistance activities are subject to any limitations imposed by law on the federal agencies in the performance of their duties.

[17] In his affidavit filed in application CSIS 10-07, Mr. Abbott described how CSEC would assist the Service if the warrant sought was issued. [

] While there is a long-standing agreement that each allied agency would treat the citizens of another allied nation as its own for the purposes of the application of its domestic legislation, Mr. Abbott acknowledged that it remained open to those agencies to pursue their own national interest with respect to the information collected.

[18] Mr. Abbott also explained how CSEC had the capability to direct activities from within Canada [

].

[19] Prior to any conclusion being reached by Justice Blanchard on the matters under consideration, in June 2007 the Supreme Court of Canada released its decision in *R. v. Hape*, 2007 SCC 26 respecting the application of the *Charter* to criminal investigations conducted in other countries by Canadian authorities.

[20] In *Hape*, the Supreme Court affirmed that Canadian legislation is presumed to conform to international law absent express statutory language to the contrary and that customary international law prohibited interference with the domestic affairs of other states. The Court found that extending the reach of the *Charter* to the actions of Canadian officials abroad would be inconsistent with those principles. The majority in *Hape* recognized, at paragraph 101, that the participation of Canadian officials abroad that would violate Canada's international human rights obligations might justify a remedy under s 24(1) of the *Charter* because of the impact of those activities on the rights of the individual in Canada.

[21] In response to questions framed by Justice Blanchard following the release of *Hape*, counsel for the Deputy Attorney General of Canada (DAGC) took the position that the scope of the Supreme Court's decision was not clear. In particular, it was submitted, it was not clear whether the Court's rationale was intended to apply, and did apply, to the conduct of security intelligence investigations outside Canada. To that extent, they argued, such investigations outside Canada might raise *Charter* issues where those investigations implicated persons having a real and substantial connection to Canada. Further, the question of whether activities outside Canada may contravene provisions of the *Criminal Code* had not been resolved, they submitted.

[22] The responsible course of action for the Service was to seek a warrant, it was argued. Should the *Charter* and the *Criminal Code* be found to be inapplicable to security intelligence investigations abroad, the worst that could occur, it was submitted, is that the warrant would have been unnecessary. The converse, should it occur, would be untenable for the Service as its officers

would continue to be exposed to *Charter* and *Code* liability if they engaged in intrusive activities without the authorization of a warrant.

[23] As discussed in my May 2009 Reasons for Order, the interception of telecommunications for which authorization was sought in the applications before Justice Blanchard in 2008 and before me in 2009 would come within the broad meaning of the term "intercept" as defined in s 2 of the Act by reference to the *Criminal Code* definition. The Service sought to listen to, record or acquire communications. Such activities constitute an "intercept" as interpreted by jurisprudence in relation to the *Criminal Code* definition: *R. v. McQueen*, (1975), 25 C.C.C. (2d) 262 (Alta. C.A.); *R. v. Giles*, 2007 BCSC 1147.

[24] Section 26 of the *CSIS Act* provides that Part VI of the *Criminal Code* does not apply in relation to any interception of a communication under the authority of a warrant issued under section 21 of the Act. Absent this protection, Part VI would apply to the interception of any "private communication" as defined by section 183 of the *Criminal Code*; that is any private communication where either the originator or the recipient was in Canada. The place of "interception" under the *Code* has been interpreted as the location where a call has been acquired and recorded: *R. v. Taylor*, [1997] B.C.J. No. 346 affirmed [1998] 1 S.C.R. 26; *R. v. Taillefer and Duguay* (1995), 100 C.C.C. (3d) 1. Thus the concern about potential liability absent a warrant or express legislative authority discussed by the DAGC in his Supplementary Submissions to the Court in the summer of 2008 was not unrealistic.

[25] Justice Blanchard issued classified Reasons for Order and Order on October 22, 2007. A public, redacted version was issued in February 2008 (*Re CSIS Act*, 2008 FC 301). Justice Blanchard described the issues before him as follows at paragraph 12 of his Reasons:

> a) Does the Federal Court have jurisdiction to issue the warrant requested?
> b) Does the Service have a mandate to undertake threat related investigations in a country other than Canada?
> c) Does the *Criminal Code*…and the *Canadian Charter of Rights and Freedoms*… apply to activities of the Service and its agents in undertaking threat related investigations in a country other than Canada?
> d) Can the Canadian [sic] Security Establishment (CSE) assist the Service in the execution of the warrant sought?

[26] The Service's rationale in support of its position that the Court had jurisdiction to issue the warrant was set out in paragraphs 22 and 23 of Justice Blanchard's decision:

> 22. The Service contends that the authorizations sought are to enable it to fulfill its mandate under section 12 of the Act. Section 12 differs from section 16 of the Act which limits the Service's collection of "foreign intelligence" to "within Canada". The Service submits that Parliament, by not imposing the same territorial limitation in section 12 as it did in section 16, must have intended its section 12 mandate to have extraterritorial reach.
>
> 23. The Service further contends that the warrant is required to ensure the Canadian agents engaged in executing a warrant abroad do so in conformity with Canadian law. The Service maintains that the warrant is required to judicially authorize activities that, absent a warrant, may breach the *Charter* and contravene the Code. This is so because the warrant powers sought to be authorized are directed at Canadians and arguably might impact on their expectation of privacy. The Service argues that the warrant would enable it to perform its duties and functions by removing the legal impediments to the conduct of a part of its security intelligence investigations outside Canada and would respect the rule of law and be consistent with the regime of judicial control mandated by Part II of the Act.

[27] On consideration of the principles of statutory interpretation, the legislative history of the Act and the principles of customary international law addressed in *Hape*, the answer to the first question was found to be negative. Absent consent of the foreign states concerned to the operation of Canadian law within their borders, the proposed investigative activities would breach their territorial sovereignty. This violation of international law could only be authorized by Parliament through express legislation. Justice Blanchard concluded, " [a]bsent an express enactment authorizing the Court to issue an extraterritorial warrant, the Court is without jurisdiction to issue the warrant sought" (paragraph 55).

[28] As a result of this determination, which was dispositive of the application, Justice Blanchard considered it unnecessary to deal with the other issues. He thought it appropriate, however, to provide his views on the third question since that had been the central focus of the Service's submissions before the Court.

[29] Justice Blanchard considered that the principles set out in *Hape* with respect to investigative actions in criminal matters were equally relevant to the collection of information in the intelligence context abroad. He concluded that the *Charter* did not apply in that context and that the offence provisions of the *Criminal Code* with extraterritorial effect were not relevant to the activities of intelligence officers collecting information abroad. In the circumstances, he was unable to find why the warrant sought would be required for the stated purpose of protecting the Service or its agents from prosecution under the Code for the limited number of offences which Parliament had defined as having extraterritorial effect (paragraph 63). It does not appear that the link between Part VI of

the *Criminal Code* and the protection afforded by s 26 of the *CSIS Act* to the interception of communications having at least one end in Canada, noted above, was raised before Justice Blanchard.

[30] In any event, nothing in Justice Blanchard's Reasons support an interpretation that CSIS officials do not need a warrant or other lawful authority, including that of the foreign state, to conduct intrusive intelligence collection activities abroad. He found, rather, that the Act did not provide for the issuance of such a warrant and that the *Charter* did not extend to such activities.

[31] In these proceedings, the Court has been provided with information about what transpired next. In the aftermath of Justice Blanchard's decision, the Director of CSIS sought further legal advice from the DAGC respecting:

> - the interception of the communications of Canadians or permanent residents who are outside Canada where the Service believes they are engaged in activities constituting a threat to the security of Canada; and
> - whether the Service can lawfully [ ] information [ ] outside Canada in cases where the Service believes the information relates to activities constituting a threat to the security of Canada and where there is a current CSIS Act warrant authorizing [ ] seizure of similar information in Canada. [underlining added]

[32] In a letter to the Director dated October 2, 2008, the DAGC set out his views on the implications of the decision in CSIS 10-07 in relation to seven factual scenarios. Several of these scenarios had not been raised in the application before Justice Blanchard and were not addressed in his decision. While these scenarios entailed the interception of communications of targets who are

outside Canada, the interceptions would take place entirely inside Canada.[

] Interceptions, [ ] and seizures conducted from within Canada, CSIS was advised, did not engage the territorial issues raised by Justice Blanchard and could properly be the subject of a warrant under s 21 of the CSIS Act given an appropriate factual context.

[33] The tasking of allied foreign agencies discussed by Mr. Abbott in his affidavit in CSIS 10-07 was briefly discussed in the opinion. This was described as the interception of a target's communications outside Canada by a foreign agency at the Service's request. Reference was not made to CSEC assistance. The DAGC stated that this did not engage the jurisdictional issues raised by Justice Blanchard and asserted that, in his view, a warrant to authorize such requests was not required. This, counsel for the DAGC now say, was based on a new interpretation of the scope of s 12 of the *CSIS Act* in light of *Hape* and Justice Blanchard's decision.

[34] The opinion respecting the scope of s 12 in the DAGC's letter of October 2, 2008 consists of no more than a bald assertion of legitimacy. The letter contains no analysis or discussion of the legislative history behind s 12 and its relationship to s 21 or other provisions of the Act read as a whole. Nor was there any discussion of the constraints placed on CSEC or the boundaries of the assistance it may provide to federal security and law enforcement agencies. The Service was cautioned that it should satisfy itself that the foreign party intercepting the communications was

acting in accordance with the laws of its own jurisdiction and that the actions of the foreign party did not give rise to serious violations of human rights. How that was to be done was not discussed.

[35] To address the Director's concern about the Service's ability to investigate threats to Canada's security by targets outside the country, the DAGC proposed that their respective officials work together to seek, by way of a fresh warrant application, an authoritative judicial interpretation of sections 12 and 21 of the Act in relation to the factual scenarios that were outside the scope of Justice Blanchard's decision. Department of Justice counsel were instructed to work with CSIS officials to identify applications on which to seek such an authorization.

[36] That opportunity arose in January 2009 in the CSIS 30-08 file. The application had been originally presented on November 27, 2008. At that time, the Court issued warrants with respect to the threat related activities of two Canadian citizens. The warrants authorized the use of intrusive investigative techniques and information collection at locations within Canada for a term of one year. On January 24, 2009 the Service sought an additional warrant as the targets were about to leave Canada and there was reason to believe that they would continue activities constituting a threat to Canada while abroad.

[37] The application was heard before me on an urgent basis on Saturday, January 26, 2009. Written submissions and authorities were filed. I was asked to revisit the question of jurisdiction and to distinguish Justice Blanchard's reasoning in the 2007 decision on the basis of a different description of the facts relating to the activities necessary to permit the interception of the

communications and the procedures to be used to obtain the information sought and a different legal argument concerning how the proposed methods of interception were relevant to the jurisdiction of this Court.

[38] In addition to the evidence of a CSIS affiant, the Service relied on an affidavit from the CSEC employee, Mr. Abbott. Mr. Abbott gave oral evidence at the hearing and was questioned closely by myself as to how the proposed methods of interception and search differed from those presented to Justice Blanchard.

[39] On the application before Justice Blanchard, Mr. Abbott's affidavit discussed in detail how the resources of the allied foreign agencies would be tasked with intercepting the communications of the Canadian travelling abroad in addition to CSEC's own collection [ ]. In his evidence before me, Mr. Abbott stated that the targeted [ ] communications and [ ] would be intercepted [ ] solely by Canadian government equipment [ ] No reference was made to tasking allied foreign agencies. There was no suggestion that CSIS or CSEC officials intended to engage the services of allied foreign agencies to assist in the collection effort. Mr. Abbott's evidence stressed that the assistance provided to CSIS would be limited to the authority granted by the warrant:

> The methods and techniques described in this affidavit could be used, were this warrant application granted, in the provision of assistance to the Service to the extent allowed by the warrant.
>
> Affidavit of James D. Abbott, January 23, 2009, para 15.

[40] After reading the material before the Court and hearing the evidence of the witnesses and the submissions of counsel, I was satisfied that there were sufficient factual and legal grounds to distinguish the application before me from that considered by Mr. Justice Blanchard and the warrant was granted. It was initially issued for a term of only three months so that I might consider the matter further. On April 6, 2009 I heard additional submissions from counsel and on April 16, 2009 I extended the warrant for a further nine months. As noted above, I issued Top Secret Reasons for Order on May 4, 2009 to explain why I believed that the Court had the jurisdiction to issue the warrant and how the application differed from that considered by Justice Blanchard.

[41] While the record is not entirely clear on this point, it appears from the information before me that no attempt was made to task foreign agencies with the collection of telecommunications intercepts in relation to the targets of the warrant issued on January 24, 2009. However, it is apparent that such actions began shortly after my Reasons for Order were issued on May 4, 2009.
[

]. They recommended that requests for assistance to the allied foreign agencies should be made at the same time as requests for assistance were made by the Service to CSEC under a 30-08 warrant. CSIS senior management agreed.

[42] The first request for assistance involving a foreign partner in addition to the scope of a 30-08 warrant was made on May 7, 2009, according to Mr. Abbott's evidence in this proceeding.

On May 27, 2009 a senior counsel of the Department of Justice Departmental Legal Services Unit at CSEC provided advice to his client that, "where a 30-08 warrant has been issued against a Canadian citizen or permanent resident located outside Canada" asking allied nations to intercept the communications of the subject of that warrant would not appear to be contrary to the CSIS Act or the *Charter*. In addition the opinion states that:

> It is understood that the warrant contains no power granted to CSIS dealing with requests to foreign nations, and that CSIS would make such request only where a warrant is in force. [Underlining added]

[43] It is not clear whether the linkage between the 30-08 warrants and the requests for foreign assistance was made at the request of CSEC officials concerned about the scope of their assistance mandate. However, it appears in a memorandum from the office of the CSIS Deputy Director of Operations on September 11, 2009 to all CSIS branch and regional offices. The memorandum stated that as a result of the Court's May 4, 2009 decision the Service could now request the Court to authorize intercepts of foreign telecommunications with the assistance of CSEC. It further states that the use of "2nd party assets will be the norm", meaning the allied foreign agencies' telecommunication collection systems. The memorandum does not state that the Court had not authorized the use of the foreign assets.

[44] While specific details would not be provided to the second parties that the individuals concerned were Service targets, the memorandum acknowledges that the second parties could infer that the collection was being conducted on behalf of the Service as it would be outside of normal practice for CSEC [ ] What they might then do with the information was beyond the control of the Service.

[45] The Court has issued more than [ ] 30-08 warrants on fresh or renewal applications since May of 2009. It appears that in the majority of these cases, if not all, CSIS has asked CSEC to task their foreign partners [

] Counsel for the Service concedes that the fact that this would be done was not disclosed in any of the applications to obtain a 30-08 warrant.

2012-2013 Annual Report of the CSEC Commissioner

[46] Commissioner Décary's 2012-2013 Annual Report was transmitted to the Minister of National Defence in June 2013. A public expurgated version was issued in late August 2013. The Public Report observed that paragraph 273.64(1) (c) of the *National Defence Act* authorizes CSEC to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. It was further noted that this would include the interception of Canadians' communications if CSIS has a judicially authorized warrant issued under s. 21 of the CSIS Act.

[47] Pursuant to subsection 273.64(3) of the *National Defence Act*, the Report noted, CSEC is subject to any limitations imposed by law on the agency to which it is providing assistance. In carrying out its other mandates, the collection of foreign intelligence and protecting Canada's electronic infrastructure, CSEC is expressly constrained from directing its activities at Canadian persons anywhere or any person in Canada and must take measures to protect the privacy of Canadian persons in the use and retention of intercepted information. Thus, the only circumstance in

which CSEC may target Canadian persons is under its assistance mandate and only then if it does so in support of another federal agency that is acting under lawful authority.

[48] The CSEC Commissioner's Annual Report contained a discussion of the Commissioner's review of CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the CSIS Act. This discussion referred to the Court's decisions in CSIS 10-07 and CSIS 30-08.

[49] The objectives of this review were described as the following at page 23 of the Public Report:

> …to acquire detailed knowledge of and to document CSEC's assistance to CSIS and to assess whether CSEC activities complied with the law, including with the terms of the warrants issued to CSIS, and any privacy protections found therein. CSEC's assistance to CSIS under the warrants may include use of Canadian identity information and the interception of the communications of Canadians. CSEC's collection, as defined in the warrant, may impact on the privacy of Canadians.

[50] The Public Report further states that the Commissioner had examined "CSEC assistance to CSIS in support of a number of the first warrants of this kind relating to counter-terrorism". The Report sets out the specific information verified by the Commissioner to assess CSEC's compliance with the law and privacy protections in this context:

- CSEC had a copy of the warrant and had clear and sufficient information about the assistance sought by CSIS;
- the communications targeted by CSEC for CSIS were only those communications referred to in the warrants;
- the communications were not targeted before the warrants came into force and were no longer targeted once the warrants expired;

- CSEC targeted the subjects of the warrants only while they were believed to be outside Canada;
- CSEC targeted only the types of communications and information that were authorized in the warrants to be intercepted or obtained; and
- CSEC complied with any other limitations imposed by law on CSIS, for example, any conditions in the warrants.

[51] In concluding this discussion, Commissioner Décary noted that he had consulted his independent counsel with respect to general questions of law relating to this subject and made two recommendations to the Minister to help ensure that CSEC assistance to CSIS is consistent with the authorities and limitations of the warrants and to enhance the measures in place to protect the privacy of Canadians. As described in the Public Report, the recommendations were that:

1. CSEC discuss with CSIS the expansion of an existing practice to protect privacy to other circumstances; and
2. CSEC advise CSIS to provide the Federal Court of Canada with certain additional evidence about the nature and extent of the assistance CSEC may provide to CSIS.

[52] Commissioner Décary concluded by observing that notwithstanding these recommendations "CSEC conducted its activities in accordance with the law and ministerial direction and in a manner that included measures to protect the privacy of Canadians." He noted that the Minister had accepted the recommendations and CSEC had raised them with CSIS. Commissioner Décary also stated that he had shared certain general points relating to CSIS that arose out of the two recommendations with the Chair of the Security and Intelligence Review Committee (SIRC).

[53] Upon reading the CSEC Commissioner's Annual Report, I issued an Order on August 26, 2013 requiring that Counsel for CSEC and CSIS appear before the Court prepared to speak to the matter. More specifically I directed that:

> …counsel should be ready to speak as to whether the application of the CSE Commissioner's recommendation "that CSEC advise CSIS to provide the Federal Court of Canada, when the occasion arises, with certain additional evidence about the nature and extent of the assistance CSEC may provide to CSIS" relates to the evidence presented to the Court in the application to obtain CSIS-30-08 and all other similar applications since, and, if yes, whether the evidence would have been material to the decision to authorize the warrant(s) in CSIS-30-08 or any subsequent applications.

[54] Counsel for CSIS and CSEC appeared before me on September 4, 2013. In preparation for that hearing, they filed a Book of Documents that included, among other things, the Reasons for Order and Order in File No. CSIS 10-07, the Reasons for Order in CSIS 30-08, the Top Secret affidavits of James D. Abbott filed on both applications and the Top Secret version of the portion of the CSEC Commissioner's Annual Report relating to the Commissioner's review of CSEC assistance to CSIS under part (c) of CSEC's mandate and sections 12 and 21 of the CSIS Act.

[55] Upon reviewing this information it became apparent to me that the focus of the Commissioner's concern was the information that had been before Justice Blanchard in the CSIS 10-07 application and was not presented in the CSIS 30-08 application or in any subsequent application for a 30-08 warrant. This was Mr. Abbott's evidence before Justice Blanchard that if the warrant was issued, CSEC would provide assistance to CSIS by, among other things, tasking its partners within the "Five Eyes" alliance (the United States, United Kingdom, Australia and New Zealand) to conduct surveillance on the warrant targets. While it was not addressed in the evidence

submitted in support of the CSIS 30-08 application, as noted above this became the default action taken by CSIS and CSEC upon issuance of a 30-08 warrant.

[56] In his Top Secret Report, Commissioner Décary summarized how the practice evolved based on the information reviewed:

[

]

[57] Commissioner Décary noted that CSEC's affidavit for Justice Blanchard discussed in detail that CSEC would use second party assets to assist in intercepting communications under 30-08 warrants, as well as how each second party partner may make use of the information that would be shared. In contrast, CSEC's affidavit and testimony in the application before me contained no information about the involvement of the second parties.

[58] In response to Commissioner Décary's inquiries about the legal grounds pertaining to 30-08 interceptions and the second parties, a letter from the Director General, Policy and Communications, CSEC dated April 12, 2011 states the following:

> … CSEC is pleased to share with the Commissioner's office copies (attached) of the six legal opinions provided to CSEC by its Directorate of Legal Services (DLS) pertaining to the interception of the communications of Canadians located outside of Canada, pursuant to a 30-08 Warrant obtained by the Canadian Security Intelligence Service (CSIS).
>
> …
>
> In relation to CSEC's legal position requesting Second Party assistance with 30-08 interception, CSEC refers the Commissioner's office to the October 2007 decision by Justice Blanchard in which he states that a warrant would not be required to authorize investigative activities outside Canada. For this reason, CSEC believes that requests for assistance to foreign nations are not within the scope of the 30-08 (in those instances where foreign assistance is provided outside Canada, the domestic law of the foreign nation applies). [Underlining added]

[59] The underlined passage is an interpretation of Justice Blanchard's October 2007 decision by CSEC legal counsel. As discussed above, there is nothing in Justice Blanchard's Reasons that states that a warrant (or express legislative authority) would not be required to authorize investigative activities outside Canada. Rather, as he declared, the Court lacked the jurisdiction under the statute to grant such a warrant. He did not address whether Parliament could authorize such activities other than by reference to the analysis in *Hape* which acknowledged that it is open to Parliament to enact such legislation.

[60] Commissioner Décary questioned whether forwarding [ ] information about the Canadian subjects of 30-08 warrants to the second parties resulted in a loss of control over the information which may result in an unauthorized violation of the subjects' reasonable expectations of privacy. CSEC officials, in response, relied on the reasoning of the majority of the Supreme Court of Canada in *Schreiber v. Canada* [1998] 1 S.C.R. 841. In *Schreiber*, the majority held that the requirement under Canadian domestic law to obtain a prior judicial authorization for a search does not apply to requesting a foreign nation to undertake an activity that could potentially engage the rights of an individual under the *Charter*, if the impugned activity was undertaken in Canada by the government of Canada. By analogy, CSEC argued, they could request that a foreign agency do within its jurisdiction that which CSIS and CSEC could not do in Canada without a warrant.

[61] In the result, Commissioner Décary accepted that Canadian law, encompassing the privacy protections contained in the *Charter*, does not apply to the interception of communications of Canadians by the second parties because they are acting within their own legal framework. He referred to this conclusion in these terms:

> Overall, the Commissioner accepts Justice Canada's and CSEC's arguments that the law can allow for second party assistance with 30-08.

[62] The DAGC relies on this conclusion but argues that Commissioner Décary's analysis as a whole is erroneous in so far as it appears to link requests for second party assistance to the 30-08 warrant authority. In my view, notwithstanding the unfortunate juxtaposition of the references to second party assistance and 30-08, Commissioner Décary understood the distinction between the

limited assistance mandate authorized by the warrant and that pursued by the Service and CSEC. In any event, Commissioner Décary's analysis, while worthy of respect, does not bind the Court.

[63] Commissioner Décary remained concerned that the second parties may decide to use the [ ] information associated with a Canadian person should one of the allies see a national interest in the subject. He noted that each of the second parties, as a sovereign nation, can derogate from the agreements made with CSEC to respect each other's laws as dictated by their own national interest.

[64] Accordingly, Commissioner Décary deemed it appropriate to recommend that CSEC discuss with CSIS an extension of its existing practice with [ ] - a caveat not to disclose or to take other action on Canadian [ ] information [ ] relating to the Canadian subjects of 30-08 warrants - to assistance with 30-08 involving CSEC's other second party partners [ ].

[65] Moreover, for clarity and to remove any ambiguities between CSEC's practices and the decision in CSIS 30-08 and because of the privacy implications of CSEC sharing with the second parties Canadian [ ] information [ ] associated with the Canadian subjects of the 30-08 warrants, Commissioner Décary believed that the Federal Court should be made explicitly aware in each case that CSEC may, at CSIS's request, share with the second party partners information about the Canadian target of a 30-08 warrant. This discussion and recommendation

appears links the issuance of a 30-08 warrant for execution in Canada and the requests made to the second parties.

[66] Having read Commissioner Décary's Secret Report and heard the preliminary submissions of counsel for CSIS and CSEC, at the conclusion of the hearing on September 4, 2013, I considered it necessary to direct that further evidence and argument be presented on two issues arising from the information before me and a hearing was scheduled for October 23-24, 2013.

[67] To assist me with the examination of these matters I appointed as *amicus curiae*, Mr. Gordon Cameron, a lawyer with the Blake, Cassels and Graydon law firm in Ottawa. Mr. Cameron is one of the Special Advocates with a Top Secret security clearance on the list maintained by the Attorney General of Canada.

[68] On October 4, 2013, counsel for the DAGC filed an affidavit from Mr. Abbott (now Director General SIGINT Programs) and written submissions together with two books of authorities. This material was also provided to Mr. Cameron and he prepared a written outline of the oral submissions he intended to make at the hearing.

ISSUES:

[69] The issues that I considered to arise from the record were:

1. Whether CSIS met its duty of full and frank disclosure when it applied for a 30-08 warrant in application CSIS 30-08 and any subsequent 30-08 warrant application; and
2. The legal authority of CSIS, through CSEC, to seek assistance from foreign partners to intercept the telecommunications of Canadians while they are outside of Canada.

Preliminary question of privilege.

[70] On October 22, 2013, counsel for the DAGC submitted an Amended Affidavit and Supplemental Affidavit from Mr. Abbott together with the affidavit of a CSIS officer, [ ] and a chronology of events. The Supplemental Affidavit and [ ]'s Affidavit were provided in a sealed envelope with the request that the Court consider oral submissions before opening and reading the documents.

[71] Appended to Mr. Abbott's Supplemental Affidavit and [ ]'s Affidavit were documents containing legal opinions provided to CSIS and CSEC by Department of Justice counsel. At the start of the hearing on October 22, 2013 I heard the oral submissions of counsel for the DAGC and the responding submissions of Mr. Cameron as to whether the documents were protected by Solicitor-Client privilege. The position taken by counsel for the DAGC was that the testimony of the affiants, Messrs Abbott and [ ] would be that in any matter pertaining to the 30-08 warrants CSIS and CSEC officials had acted on the advice of their lawyers. The appended documents would demonstrate that was the case, I was told. It was submitted, however, that the specific content of that advice remained privileged. The *amicus* responded that any privilege

attaching to the documents was implicitly waived by the assertion of legal advice as the justification for the actions of CSIS and CSEC officials.

[72] Counsel for the DAGC invited me to review the material and determine whether privilege attached to the content of the documents. Accordingly, I recessed to read the documents and consider the matter. Upon resuming the hearing, I indicated that I was satisfied that the content was not privileged.

[73] As argued by the *amicus*, waiver may implicitly result from reliance on privileged communications in litigation: Robert W. Hubbard et al, *The Law of Privilege in Canada*, (Toronto: Thomson Reuters 2013) ch 11 at 64. Thus in *R. v. Campbell*, [1999] 1 S.C.R. 564 at para 67, it was found that where the holder of privilege relies upon legal advice to justify the legality of his or her actions, they have "waived the right to shelter behind solicitor client privilege the contents of the advice thus exposed and relied upon."

[74] I considered, however, that it was not necessary to share the entire content of one document attached to Mr. Abbott's Supplemental Affidavit with the *amicus*; that being the opinion provided by the DAGC to the Director of CSIS in October, 2008 which I have discussed above. While that document provided useful information about the background to the issues, its disclosure to the *amicus* in full was not necessary for him to assist me in the determination of the issues. I read what I considered to be the most relevant portion of the opinion into the record – that related to the interpretation of s 12 of the *CSIS Act*. The affidavits and the other appended documents were then

entered as received at the hearing and, apart from the October 2008 opinion, disclosed to Mr. Cameron. Messrs Abbott and [ ] were then called as witnesses and examined as to their knowledge of the circumstances giving rise to the applications for CSIS 10-07, CSIS 30-08 and subsequent warrants.

ARGUMENT AND ANALYSIS:

Did CSIS meet its duty of full and frank disclosure when it applied for a 30-08 warrant in application CSIS 30-08 and any subsequent30-08 warrant application?

[75] As I have noted above, on the record before me it is not clear that a request for foreign assistance was made in application CSIS 30-08 although that might be inferred from the timing of the first request just days after my Top Secret Reasons for Order were released, according to Mr. Abbott's evidence. The DAGC agreed, however, that the issue should not be resolved on the basis that there was no actual non-disclosure in CSIS 30-08. The DAGC acknowledges that there was no disclosure of the requests for foreign assistance in the applications that followed the rationale developed in CSIS 30-08. Rather than have the matter addressed in each of those files, the DAGC agreed that the issue ought to be dealt within a single proceeding.

[76] In his testimony, Mr. Abbott candidly stated that his evidence in CSIS 30-08 was "crafted" with legal counsel to exclude any reference to the role of the second parties described in his affidavit before Justice Blanchard.[

]

[77] While discussions had been ongoing between CSIS and CSEC prior to the January 2009 application about the implications of Justice Blanchard's decision, Mr. Abbott stated that he was not aware of any actual requests for second party assistance prior to the issuance of the first 30-08 warrant:

> Yes, they would have been in the context of 30-08 warrants from January of 2009 when we receive the first signed warrant from the Federal Court. This is the first instance where they requested that we utilize second party assets to target that individual while he was outside of Canada. (Transcript, October 23, 2013 pp. 42-43)

[78] In his Amended Affidavit dated October 22, 2013, Mr. Abbott disclosed that in relation to the individuals who were subject to a 30-08 warrant over the preceding 12 months, [

].

[79] The DAGC contends that the Service met its duty of full and frank disclosure when it sought a 30-08 warrant in application CSIS 30-08 and in all subsequent applications for such a warrant. It is argued that the Service provided all material information in these applications and the fact that the Service may request assistance from foreign partners through CSEC to intercept the telecommunications of Canadians abroad is not an issue properly before this Court on warrant applications.

[80] The view of the *amicus* is that there was a serious breach of the duty of candour to the court in the CSIS 30-08 application and in the subsequent applications that relied on that decision. That breach has been exacerbated, the *amicus* submits, by the failure to acknowledge the lack of candour in this proceeding because it demonstrates that the Service does not understand its duty when it comes before this Court *ex parte*.

[81] The information about the requests to foreign agencies was relevant to the application in CSIS 30-08 and subsequent applications, the *amicus* submits, because, if correct, the Service has an alternative means of investigation that paragraph 21 (2) (b) of the Act requires be disclosed to the judge hearing the warrant application. The application in CSIS 30-08 and the subsequent applications for 30-08 warrants were calculated, he submits, to have the Court understand the opposite of what was put before Justice Blanchard. The applications were crafted to give the Court the impression that the only interceptions of the target's communications would be [

] Canada under authority of the warrant. It was solely on this basis that the

Court concluded that it had jurisdiction to issue a warrant. Had the information been disclosed, the Court may have reached a different conclusion.

[82] The duty of full and frank disclosure in an *ex parte* proceeding was discussed by the Supreme Court of Canada in *Ruby v Canada (Solicitor General)* 2002 SCC 75, [2002] 4 S.C.R. 3 at para 27:

> In all cases where a party is before the court on an *ex parte* basis, the party is under a duty of utmost good faith in the representations it makes to the court. The evidence presented must be complete and thorough and no relevant information adverse to the interests of that party may be withheld; *Royal Bank*, *supra*, at paragraph 11. Virtually all codes of professional conduct impose such an ethical obligation on lawyers. See for example the *Alberta Code of Professional Conduct*, c.10, r.8.

[83] The DAGC acknowledges that this duty, also known as the duty of utmost good faith or candour, applies to all of the Service's *ex parte* proceedings before the Federal Court: *Harkat (Re),* 2010 FC 1243 at para 117, rev'd on other grounds 2012 FCA 122, appeal on reserve before the Supreme Court; *Charkaoui (Re),* 2004 FCA 421 at paras 153, 154; *Almrei (Re),* 2009 FC 1263, para 498. In making a warrant application pursuant to sections 12 and 21 of the *CSIS Act*, the Service must present all material facts, favourable or otherwise.

[84] It is submitted on behalf of the Service that:

> …the fact that in addition to seeking warrants from the Court the Service may also seek the assistance, through CSEC, of foreign partners to intercept under their own legal framework telecommunications of a Canadian subject of investigation abroad as

> part of a lawful investigation in Canada is not a material fact which could have been relevant to the designated judge in making determinations required for the purpose of exercising a discretion in the context of a warrant application pursuant to section 21 of the *CSIS Act*.

[85] In advancing this argument, the DAGC relies on definitions of "material facts" set out in decisions relating to criminal proceedings. In the context of a criminal trial, evidence is material if what it is offered to prove or disprove is a fact in issue as determined by the allegations contained in the indictment and the governing procedural and substantive law: *R.v. Luciano*, 2011 ONCA 89 at para 207.

[86] It is submitted by the DAGC that in the context of a warrant application, materiality refers to information that is probative to the legal or factual determination that a judge will be asked to make when deciding whether to grant or deny the request for a warrant: *R. v. Lee*, 2007 ABQB 767, at paras 132-136. The lack of any reference to requests for assistance to foreign partners was not included in 30-08 warrant applications because it was legally and factually irrelevant to the issuance of the warrant sought, it is argued. This Court's jurisdiction, as determined by Mr. Justice Blanchard, did not extend to governing the relationship between the Service and the foreign partners, the DAGC submits.

[87] In *R.v. G.B.*, [2003] O.T.C. 785 (Ont. S.C.J.), a case involving an application for a stay of proceedings on the ground that a police officer had lied in affidavits to obtain wiretap authorizations, the Court described material facts as follows at paras 11 and 12:

> 11… Material facts are those which may be relevant to an authorizing judge in determining whether the criteria for granting a wiretap authorization have been met. For the disclosure to be frank, meaning candid, the affiant must turn his or her mind to the facts which are against what is sought and disclose all of them which are known, including all facts from which inferences may be drawn. Consequently, the obligation of full and frank disclosure means that the affiant must disclose in the affidavit facts known to the affiant which tend to disprove the existence of either reasonable and probable grounds or investigative necessity in respect of any target of the proposed authorization.
>
> 12. The obligation of full and frank disclosure also means that the affiant should never make a misleading statement in the affidavit, either by means of the language used or by means of strategic omission of information. [Underlining added]

[88] I agree with counsel for the DAGC that in the context of a warrant application pursuant to section 21 of the *CSIS Act*, material facts are those which may be relevant to a designated judge in determining whether the criteria found in paragraphs 21 (2) (a) and (b) have been met. The criteria are as follows:

> 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;
> b) that other investigative procedures have been tried and had failed and 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 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.

[89] However, I do not accept the narrow conception of relevance advocated by the DAGC in this context as it would exclude information about the broader framework in which applications for the issuance of *CSIS Act* warrants are brought. In my view it is tantamount to suggesting that the Court should be kept in the dark about matters it may have reason to be concerned about if it was made aware of them. In the circumstances under consideration that would include matters relating to the prior history of attempts to have the Court authorize the collection of security intelligence abroad and the potential implications of sharing information about Canadian persons with foreign security and intelligence agencies.

[90] Based on the documentary record before me and Mr. Abbott's evidence, I am satisfied that a decision was made by CSIS officials in consultation with their legal advisors to strategically omit information in applications for 30-08 warrants about their intention to seek the assistance of the foreign partners. As a result, the Court was led to believe that all of the interception activity would take place in or under the control of Canada.

[91] Mr. Abbott certainly understood the importance of providing the Court with information about the process "so that the Court would have a good understanding of how these activities would be undertaken." On cross-examination he observed that:

> … if we are seeking this assistance, the Court should be aware of what the second party agency would see and what they may or may not choose to do with that information. (Transcript, October 23, 2013 p. 59)

[92] It was a material omission for the Service not to explain its new, different and never articulated to the Court theory that, contrary to its position before Justice Blanchard, it did not require warrant authority to task the assets of the second party allied nations to conduct foreign interceptions. That leads me to the second issue.

Does CSIS have the legal authority to seek assistance, through CSEC, from foreign partners to intercept the telecommunications of Canadians while they are outside of Canada?

[93] In the CSIS 10-07 application before Justice Blanchard, the Service's main contention was that the warrant sought was required to ensure that Canadian agents engaged in [

] abroad did so in conformity with Canadian law since the impugned investigative activities may, absent the warrant, breach the *Charter* and contravene the *Criminal Code*. At that time they argued that a warrant could be issued under s 21 of the Act. This approach would respect the rule of law and would be consistent with the regime of judicial control mandated by Part II of the Act, they submitted.

[94] The Service contends now that they accepted the outcome of Justice Blanchard's decision and, in particular, his finding that the Court had no authority to issue such a warrant. In light of that, they say, they turned to the general authority to investigate threats to the security of Canada set out in s 12 of the Act. They reached the conclusion, through the advice of their legal counsel, that a warrant was not required for CSIS to engage the assistance of the second parties through CSEC to intercept the private communications of Canadians outside the country. CSEC, they argue, does not

breach the prohibition against targeting Canadians in the *National Defence Act* when it provides assistance to CSIS operating under the general investigative authority granted the Service by s 12.

[95] On the record before me it appears that no attempt was made to rely on s 12 as the lawful authority required by CSEC to target Canadians in the exercise of its Part C assistance mandate until the spring of 2009 after the Court had issued the first 30-08 warrant.

[96] In the view of the *amicus*, the Attorney General's interpretation of the scope of s 12 of the Act allows the Service "to contract out interceptions of Canadians' communications or accessing Canadians' information without any warrant or supervision by this Court". Mr. Cameron characterized this as "effectively an end run around s 21 and following of the Act." He submitted, however, that I did not have to decide the issues of the scope of s 12 of the Act, or this Court's jurisdiction to issue a warrant for CSIS through CSEC to seek lawful assistance from second party countries, in addressing the breach of candour.

[97] In my view, it is necessary for the Court to express an opinion on the matter in light of the public association, through the CSEC Commissioner's Report, between the issuance of the 30-08 warrants by the Court and the requests for second party assistance. As I will discuss below, that public association has been further highlighted by the recent publication of the Annual Report of the Security Intelligence Review Committee ("SIRC"). The Court must be concerned that the authority granted it by Parliament to authorize intrusive investigative activities by the Service may be

perceived in the public arena as approving the surveillance and interception of the communications of Canadian persons by foreign agencies.

[98] S 12 of the *CSIS Act* reads as follows:

> The Service shall collect, by investigation or otherwise, to the extent that it is strictly necessary, and analyze 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.
>
> ---
>
> 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.

[99] Section 12 gives the Service the authority to conduct investigations, collect, analyse and retain information and report to the Government of Canada respecting any activities which may reasonably be suspected of constituting threats to the security of Canada. The scope of the power granted by s 12 must be read in conjunction with the scheme of the Act, the guarantees and protections set out in the *Charter* and any limitations imposed under domestic law such as the *Criminal Code*.

[100] Section 12 does not give the Service an exemption from the operation of these laws of general application. Where required, the Service may seek the authority of a warrant under s 21 to engage in investigative methods that would otherwise constitute a crime or a breach of the *Charter*

guarantee against unreasonable search and seizure. As discussed above, s 26 provides that Part VI of the *Criminal Code* does not apply to any interception of a communication under the authority of a warrant issued under s 21 or in relation to any communication so intercepted. Absent such protection, Service personnel are exposed to liability under Part VI of the Code in relation to the interception of any communication that has a Canadian end.

[101] The DAGC points to Commissioner Décary's conclusion that the second parties can intercept communications of Canadian subjects of a 30-08 warrant because they are acting within their own legal frameworks. Canadian law cannot either authorize or prohibit the second parties from carrying out any investigation they choose to initiate with respect to Canadian subjects outside of Canada. That does not exempt Canadian officials from potential liability for requesting the interception and receiving the intercepted communication. I recognize that it is unlikely that this would actually result in charges against CSIS or CSEC personnel. However, the potential for the issue to arise with respect to the admissibility of any intercepted communication or derivative evidence in a subsequent prosecution against the targets or as the basis of an action for a remedy under the *Charter* is, I believe, realistic. As noted above, the Supreme Court did not close the door in *Hape* to a remedy under s 24 (1) of the *Charter* where the result of the actions of Canadian officials abroad has an impact on the exercise of *Charter* rights in Canada.

[102] Section 12 does not expressly authorize the Service to invoke the interception capabilities of foreign agencies. While such interception may be lawful where it is initiated under the domestic legislation of the requested state, such as the *Foreign Intelligence Surveillance Act of 1978*, Pub.L.

95-511, 92 Stat. 1783, 50 U.S.C. ch.36 (*FISA)*, it may be unlawful in the jurisdiction where the interception actually occurs. *FISA*, as amended, permits warantless searches for foreign intelligence collection as authorized by the President and the surveillance of foreign subjects under court order. *FISA* thus authorizes the violation of foreign sovereignty in the manner which the Supreme Court of Canada in *Hape* recognized as contrary to the principles of customary international law but permissible under domestic law – express legislative authority.

[103] There is nothing in the *CSIS Act* or in its legislative history, to my knowledge, that suggests that in enacting s 12 Parliament granted express legislative authority to CSIS to violate international law and the sovereignty of foreign nations either directly or indirectly through the agency of CSEC and the second parties.

[104] The DAGC submits that the decision of the Supreme Court of Canada in *Schreiber*, above, is a complete answer to the question of whether a request can be made to a foreign agency to provide information about a Canadian person. But in *Schreiber*, the foreign agency was asked to provide information in conformity with its own laws and in the exercise of its own territorial sovereignty. There was no suggestion in *Schreiber* that in acting upon such a request, the foreign jurisdiction would violate the sovereignty of any other nation, as there is, implicitly, here.

[105] As discussed by the Supreme Court in *Hape* at paragraphs 51, 52 and 101 and in *Canada (Justice) v Khadr*, 2008 SCC 28 at paragraph 18, the principle of comity between nations that implies the acceptance of foreign laws and procedures when Canadian officials are operating abroad

ends where clear violations of international law and human rights begin. In tasking the other members of the" Five Eyes" to intercept the communications of the Canadian targets, CSIS and CSEC officials knew, based on the legal advice that they had been given about the implications of *Hape* and Justice Blanchard's decision, that this would involve the breach of international law by the requested second parties.

[106] CSEC is expressly prohibited under the legislation adopted in 2001 by Parliament from targeting Canadian persons unless it is done under its mandate to assist federal law enforcement and security agencies in the performance of their lawful duties and subject to any limitation imposed by law on those agencies. In this context, CSEC has no greater authority than that conferred upon CSIS.

[107] The record before me indicates that CSEC consistently interpreted Parliament's references to "lawful duties" and "limitation imposed by law" in the 2001 amendments to the *National Defence Act* as requiring a warrant. The legal advice given to CSEC in May 2009 stipulated that CSIS would make a request for second party assistance only where a warrant was in place. To Mr. Abbott's knowledge, the Service had never made a request for second party collection unless they have had a parallel authority in the form of a warrant. To his recollection, there had never been a discussion between the two agencies about the use of s 12 as the sole ground of lawful authority for CSEC to assist CSIS in its investigation by tasking the second party [ ].

> … If they were to come to us and it wasn't a parallel 30-08 warrant, we would then have a very -- I will use the words serious discussion with our legal counsel and with the Service as to if this was the first time we were going to do this, let's make sure everybody is clear and

> understands, as I said earlier, based on the legal advice that we received to date, legally my understanding of what we had been told is we could do that.
>
> Transcript, October 23, 2013 pp 80-81.

[108] [ ] , the CSIS witness who was responsible for the warrant process in 2009, also acknowledged that CSIS looked primarily to the judicial warrants issued by this Court for the authority to ask CSEC to request the assistance of the second parties to intercept and collect the communications of Canadians. Neither agency appears to have been prepared to proceed solely on the strength of the DAGC's October 2008 opinion. The 30-08 warrants gave the officials of both agencies comfort that they were acting within the scope of their lawful authority.

[109] The DAGC acknowledges this and submits that the power under s 12 is broader than what CSIS and CSEC have previously chosen to exercise. It is appropriate, it is argued, that the two agencies decided to proceed only where a 30-08 warrant has been issued. The process of establishing judicial authority for the 30-08 warrant shows that they have gone before a court, established on reasonable grounds that the activities of the particular individual or individuals are believed to be a threat to the security of Canada and that they are going to be traveling outside Canada's borders. This shows respect for the rule of law, the DAGC contends.

[110] While that may be the case, it is clear that the exercise of the Court's warrant issuing authority has been used as protective cover for activities that it has not authorized.

[111] The DAGC's interpretation of the scope of s 12 of the *CSIS Act* provided to the Service in October 2008 is, in my view, highly questionable. There is nothing in any of the material that I have read or in the oral submissions of counsel for the DAGC that persuades me that it was the intent of Parliament to give the Service authority to engage the collection resources of the second party allies to intercept the private communications of Canadians under the general power to investigate in s 12. Moreover, I have reviewed the legislative history of the amendments to the *National Defence Act* in 2001 and found nothing that would suggest that Parliament had contemplated that CSEC could extend such assistance to CSIS solely under the authority of s 12.

[112] I am satisfied that the Service and CSEC chose to act upon the new broad and untested interpretation of the scope of s 12 only where there was a 30-08 warrant in place. My view of the matter has been reinforced by the publication on October 31, 2013 of the 2012 – 2013 Annual Report of the Security Intelligence Review Committee. A section of the report refers to a review of CSIS's "Review of a new section 21 warrant power". A copy of the classified version of that study was provided to the Court by counsel to the DAGC by letter dated November 6, 2013 as it had been referenced during the hearing on October 23 and 24, 2013.

[113] SIRC reported on what it described in the public report as "a new warrant power under section 21 of the CSIS Act which was initially authorized by the Federal Court in 2009". The discussion of this review in the public report includes the following statements:

> During the review period, 35 warrants (+7 supplemental warrants) that included the new power were issued… by relying on partner agencies-both domestic and foreign-for collection some efficiency will ultimately be sacrificed. There has been substantial progress since the first warrant was issued; however, CSIS is still in the learning phase and it will need to manage expectations against the realities, meaning limitations, of reporting from this collection.
>
> In order to maximize collection under the new warrant power, CSIS, in almost every case, leverages the assets of the Five Eyes community (Canada, plus the United States, the United Kingdom, Australia and New Zealand). SIRC noted that even with the assistance of allies, the collection or intelligence yield under this power has provided different gains and challenges than the Service initially expected.

[114] The classified version contains additional statements that I consider relevant to this matter:

[

]

[115] These passages suggest that SIRC is operating under the mistaken impression that the 30-08 warrants issued by this Court authorize the collection of intercepts respecting Canadian persons by foreign agencies. In doing so, the Court is associated with the concern identified by SIRC that the ability of a Five Eyes partner to act independently on CSIS originated information carries the risk of the detention of or other harm to a Canadian person based on that information. Both Commissioner Décary and SIRC have recognized in their reports the hazards related to the

lack of control over intelligence information once it has been shared. Given the unfortunate history of information sharing with foreign agencies over the past decade and the reviews conducted by several Royal Commissions there can be no question that the Canadian agencies are aware of those hazards. It appears to me that they are using the 30-08 warrants as authorization to assume those risks.

CONCLUSION:

[116] The Service, acting on the advice of the Department of Justice, sought authorization from the Court to engage in security intelligence activities outside of Canada for which they require a warrant if conducted in Canada. The Service and their counsel were told by the Court that it lacked the jurisdiction to issue a warrant for such purposes under s 21 of the *CSIS Act*. They then returned to the Court with a new rationale for the issuance of a warrant based on the clearly stated grounds that the proposed interceptions [ ] would be carried out from within Canada and controlled by Canadian government personnel. Having obtained authorization under warrant to conduct such interceptions [ ] from and under the control of Canada, they engaged the assistance of second party foreign allies [ ] and failed to inform the Court that this was being done on any of the subsequent applications.

[117] In my view, as soon as it was determined that the Service would rely on the general power to investigate set out in s 12 of the Act to request second party assistance with the interception of the communications of Canadian subjects abroad, that determination constituted facts known to the

affiant which could lead the Court to find that there was no investigative necessity to issue a 30-08 warrant. The failure to disclose that information was the result of a deliberate decision to keep the Court in the dark about the scope and extent of the foreign collection efforts that would flow from the Court's issuance of a warrant.

[118] This was a breach of the duty of candour owed by the Service and their legal advisors to the Court. It has led to misstatements in the public record about the scope of the authority granted the Service by the issuance of the 30-08 warrants.

[119] The conclusion reached in application CSIS 30-08 that the Court has the jurisdiction to issue a warrant under s 21 for the domestic interception of foreign telecommunications under certain defined conditions remains valid in my view. That jurisdiction does not extend to the authority to empower the Service to request that foreign agencies intercept the communications of Canadian persons travelling abroad either directly or through the agency of CSEC under its assistance mandate.

[120] Parliament has given the Minister of National Defence the power to approve foreign intelligence collection activities in respect of certain classes of activities. The legislative authority for CSEC to carry out its functions under the *National Defence Act* does not extend to the specific targeting of Canadian persons. CSEC may only do so in the exercise of its assistance mandate when the assisted federal law enforcement or security agency is acting under lawful authority. In my view,

in enacting s 12, Parliament did not contemplate that it would be used by CSIS and CSEC to engage the interception capabilities of foreign agencies against Canadian persons.

[121] It is open to Parliament, as discussed above, to amend the statute to enable the Court to authorize foreign interception. Authorization by an independent judicial officer on a particularized warrant application would ensure that any rights that the individual subjects may have would be respected and would also extend protection to the officials of the concerned agencies from potential liability so long as they were operating within the scope of the authority granted. Absent amendment to the statute, however, the Court does not have that jurisdiction.

[122] The interpretation of s 12 asserted by the Service and the DAGC is not, I believe, consistent with the scheme of the Act as a whole nor with the position of the Supreme Court of Canada in *Hape* that the violation of international law can only be justified if expressly authorized by Parliament. CSIS and CSEC officials are relying on that interpretation at their peril and, as cautioned by the CSEC Commissioner and SIRC, incurring the risk that targets may be detained or otherwise harmed as a result of the use of the intercepted communications by the foreign agencies. Section 12 does not authorize the Service and CSEC to incur that risk or shield them from liability, in my view.

[123] I express no opinion on the status of any information already collected by the Service as a result of its interpretation of s 12 of the Act and the requests for assistance to the second party

agencies that it has made since 2009 through CSEC. That question may yet need to be addressed by this or another Court.

[124] Going forward, where an application is made to the Court for a 30-08 warrant, the Court must be informed whether there has been any request for foreign assistance and, if so, what the results were in respect of the subjects of the application. In such circumstances, the Court should consider whether the investigative necessity for the issuance of the warrant has been established. I note in that regard, that the classified SIRC report questions the effectiveness of the 30-08 collection activities. Such information should be disclosed to the Court on each application for the Court to determine whether it is necessary to issue the warrant.

[125] It must be made clear, in any grant of a 30-08 warrant, that the warrant does not authorize the interception of the communications of a Canadian person by any foreign service on behalf of the Service either directly or through the assistance of CSEC. To that end, an appropriately worded limitation must be added to the text of the warrant.

[126] There must be no further suggestion in any reference to the use of second party assets by CSIS and CSEC, or their legal advisors, that it is being done under the authority of a s 21 warrant issued by this Court.

[127] A copy of these Further Reasons for Order will be provided to the Chair of SIRC and to the CSEC Commissioner. The Service will be given two weeks to comment on the public release of

these Further Reasons for Order. A public summary will be issued with prior notice to the Service and to the Attorney General.

"Richard G. Mosley"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CSIS-30-08
STYLE OF CAUSE:	IN THE MATTER OF an application by [ ] for a warrant pursuant to Sections 12 and 21 of the *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23; AND IN THE MATTER OF [ ]
PLACE OF CLOSED HEARING:	OTTAWA, ONTARIO
DATES OF CLOSED HEARING:	SEPTEMBER 4, 2013, AND OCTOBER 23-24, 2013
REDACTED AMENDED FURTHER REASONS FOR ORDER:	MOSLEY, J.
DATED:	NOVEMBER 22, 2013

APPEARANCES:

Mr. Robert Frater Ms. Isabelle Chartier Mr. Jacques-Michel Cyr Mr. Rémi Chapadeau	FOR THE APPLICANT DEPUTY ATTORNEY GENERAL OF CANADA
Mr. Gordon Cameron	AMICUS CURIAE

SOLICITORS OF RECORD:

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

Blakes Law Firm
Ottawa, Ontario

AMICUS CURIAE