Federal Court Cour fédérale

~~**TOP SECRET**~~

Date: 20200515

Docket: CONF-1-20

Citation: 2020 FC 616

Ottawa, Ontario, May 15, 2020

PRESENT: The Honourable Mr. Justice Gleeson

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

AND IN THE MATTER OF Islamist Terrorism,
[redacted]

JUDGMENT AND REASONS

TABLE OF CONTENTS

I. Overview

[1] Can a designated judge considering whether to issue a warrant under section 21 of the *Canadian Security Intelligence Service Act*, RSC 1985, c. C-23 [*CSIS Act*] rely on illegally collected information? If yes, what factors should the designated judge take into account? These questions are novel and important.

[2] Whether the Canadian Security Intelligence Service [CSIS or the Service] or its agents have illegally collected information relied on in a warrant application is also highly relevant to the exercise of a designated judge's discretion to issue the warrant or not.

[3] Regrettably, in recent warrant applications, neither the Service nor counsel for the Attorney General of Canada [AGC] brought the issue of illegally collected information to the Court's attention. Instead, the issue surfaced as the result of Justice Simon Noël's inquiries in warrant application [Case A]

[4] The Service's and counsel's failure to identify the issue of information that has been potentially illegally collected—an issue directly relevant to the judicial assessment of the application—calls into question the commitment and ability to comply with the duty of candour. How and why did such a fundamental breach of the duty to fully and frankly disclose to the Court all information relevant to the application occur? What consequences flow from this breach?

[5] As this proceeding unfolded and the issue of illegality crystalized, the Service advised the Court that it had relied on potentially illegally collected information in at least two other warrant applications: [Case C] before Justice Catherine Kane and [Case D] before Justice Henry Brown. This spawns additional issues. May a designated judge invalidate an issued warrant where it is subsequently discovered that the Service has breached its duty of candour by not disclosing potential illegality? What is the impact upon the retention and use of information collected under a warrant invalidated in these circumstances?

[6] On receiving notice of these issues, Justice Richard Mosley, who at that time was the coordinating judge of designated proceedings, convened an *en banc* hearing in February 2019. This was followed by common issues hearings presided over by the designated judges seized with the three applications impacted by illegality: myself (having taken carriage of [Case A] from Justice Noël), Justice Kane, and Justice Brown. Throughout most of 2019, sitting together but individually seized, we heard evidence and received submissions common to all three applications—namely, the candour breach and the circumstances that permitted it.

[7] Mr. Gordon Cameron and Mr. Matthew Gourlay have been appointed *amici* in [Case B] the *en banc* hearing, and the common issues hearings.

[8] These reasons are lengthy. I begin with a general overview of the proceedings and then provide background relating to (1) the issue of illegality and how it arises in these matters; (2) Service processes where the issue of potentially illegal collection activities should have been identified but was not; and (3) legislative reforms that were pursued to address illegality on a going forward basis. After identifying the numerous legal issues that arise in this matter I then consider each of those issues. Finally, I address the specific issues that arise from [Case A] and [Case B].

[9] In the course of these proceedings the Director of the Service waived solicitor-client privilege over legal advice provided to the Service as it related to the issues of Crown immunity and illegality within this context. In the course of oral submissions it was suggested by AGC counsel that the waiver was not entirely voluntary. Although provided the opportunity to do so counsel did not advance further argument in this regard. However, in light of the fundamental importance of solicitor-client privilege I briefly address the circumstances at the conclusion of this judgment.

II. Proceedings

[10] The issues before me arise from the Service's application for warrants under sections 12 and 21 of the *CSIS Act* in furtherance of its investigation of Islamist Terrorism and the [redacted]

proposed warranted subjects of investigation identified in the style of cause. The Service filed this application in March 2018 under court file [Case A].

A. *[Case A]*

[11] Justice Noël was initially seized with this application. In April 2018, he presided over an *ex parte* hearing. There, he identified areas of concern, which included the Service's collection activities described in the supporting affidavit and the reference to one of the [redacted] targets as an [redacted]. In addition, he queried whether funds that the affiant reported had been paid to an individual "could be used for terrorist activities," noting that the "*Criminal Code* talks about that."

[12] Justice Noël was not satisfied with the responses provided to many of his questions. AGC counsel undertook to provide additional information. Ultimately, in considering the application, Justice Noël excluded all information obtained through the collection methods he had questioned or that was related to other identified areas of concern. After doing so, he concluded that sufficient reliable information remained to satisfy the requirements of section 21 of the *CSIS Act*. Justice Noël issued the warrants, but remained seized of the application for the purpose of dealing with the undertakings.

[13] AGC counsel's response to the undertakings triggered further exchanges with the Court and a case management conference [CMC] was held in May 2018. In June 2018, new AGC counsel assumed carriage of the file and wrote to the Court to acknowledge errors and omissions

in the application including the human source précis. To address these, counsel proposed that the Service file a fresh application against the same subjects. Counsel subsequently confirmed that the errors and omissions did not relate to the information that Justice Noël relied on to issue the warrants.

[14] Justice Noël requested that the Chief Justice reassign the matter and I took carriage of the file in June 2018.

[15] In July 2018, in a CMC, AGC counsel confirmed the Service's intention to file a fresh application that would be more complete and address the identified deficiencies of the initial application. Counsel took the position that the fresh application would serve two purposes. It would create a single record of relevant information that had previously been provided in various forms. It would also provide a venue to hear full evidence and argument on the important issues identified in [Case A].

B. *[Case B]*

[16] In September 2018, the Service filed the fresh application: [Case B]. In October 2018, at the hearing of the application, I concluded that resolution of the outstanding issues from [Case A] was relevant in determining what was to be considered in support of the application. The [Case A] warrants remained in force. I therefore reserved on determining the application pending consideration of the underlying legal issues.

[17] In November 2018, I heard submissions for the purpose of defining the legal questions arising out of [Case A] and [Case B]. In December 2018, I issued a Direction which set out the issues for the AGC and the *amici* to address. As described below, the candour and illegality issues evolved significantly through January and February of 2019. It became clear that the outstanding issues from [Case A] would require some time to fully address.

[18] In April 2019, I heard updated evidence and submissions in [Case B]. After excluding from consideration the information identified in my Supplemental Order of April 4, 2019, I was satisfied that the remaining evidence met the requirements of section 21 of the *CSIS Act*. The requested warrants were granted and remained in force until July 5, 2019. In granting the warrants I remained seized of the application for the purpose of addressing the outstanding issues.

C. *Notice to the Court*

[19] On January 18, 2019, the Senior General Counsel for the National Security Litigation and Advisory Group [NSLAG]—the group within the Department of Justice responsible for representing and advising the Service—wrote to the Court. The letter advised that in the course of preparing renewal and supplemental applications for warrants the Service realized that some information that was relied on in two separate applications—[Case C] before Justice Kane and [Case D] before Justice Brown—was derived from potentially illegal activities. Warrants had been issued in both applications. The letter also advised that the Service was conducting a review to determine whether this issue arose in other circumstances.

[20] The letter enclosed a document entitled “Interim Direction on the Conduct of Operations Likely Involving the Commission of Criminal Offences.” The Deputy Director Operations for the Service issued this document the day before the Senior General Counsel wrote to the Court. It indicated that the Service would no longer approve operations that were likely illegal—characterized as posing a “high legal risk”—and that the Service would review any such operations that were ongoing to mitigate potential illegality.

D. *January 2019 case management conference*

[21] In response to the Senior General Counsel’s letter, Justice Mosley, as coordinating judge of designated proceedings at the time, convened a CMC on January 21, 2019. The CMC was conducted by him and Justice Kane as Chief Justice Crampton, Justice Brown and I were not in Ottawa at that time. The Senior General Counsel for the NSLAG appeared on behalf of the Service. He confirmed that the illegality involved conduct by the Service or human sources acting on its direction that was likely contrary to the anti-terrorism provisions of the *Criminal Code*, RSC 1985, c. C-46 [*Criminal Code*]; that the Service had isolated in its databases information collected under the authority of the warrants issued by Justice Kane and Justice Brown; that although collection in these matters was ongoing, information collected under the warrants was being reviewed only to the extent necessary to determine if it disclosed an imminent danger; and that the Service was conducting a review to determine if information relied on to obtain any other active warrants had been collected through illegal activity.

E. *En banc hearing*

[22] Further to the January 18 letter and the January 21 CMC, on January 29, 2019 Justice Mosley ordered an *en banc* hearing. In doing so, he noted the illegality issues identified by the Service and additional affidavit evidence filed in [Case B] on January 25, 2019.

[23] The additional evidence in [Case B] included two affidavits of documents that impact upon the broader issues that arise in this matter.

[24] The first stated that the Director of the Service had waived solicitor-client privilege over six documents containing legal opinions addressing whether the Service benefited from Crown immunity. Attached as exhibits are three of those opinions. Notably: one opinion from January 2017 and another opinion from January 2019, both of which conclude that the Service could not breach the *Criminal Code* under the guise of Crown immunity.

[25] The second included the remaining three legal opinions over which solicitor-client privilege has been waived. These opinions are embedded in the documentation that evidences the Service's review and approval of operations involving human sources.

[26] On February 21, 2019, the *en banc* hearing proceeded before all available designated judges. Those judges seized with the applications in issue presided to the extent that the *en banc* engaged questions relating specifically to those applications. At the outset of the hearing, the

Chief Justice explained that the Court's goal was to gain an understanding of the "broader issues" common to all three applications and the "potential implications" of these issues for other warrants.

[27] The *en banc* hearing confirmed that candour and illegality issues were common to the matters before myself, Justice Kane, and Justice Brown, and that evidence would be required to address the common issues. AGC counsel advised that it would file additional evidence to provide detail on the issue of illegality in each file, and to address the state of knowledge in both the Service and the Department of Justice in respect of that illegality.

F. *Chief Justice's initial direction*

[28] After the *en banc* hearing, the Chief Justice issued a Direction as an initial response to the Court's candour concerns and to highlight the importance of the duty of candour. The Direction reiterates that the Service is bound by the duties of candour and utmost good faith and notes that the evidence as disclosed to that point suggested that the non-disclosure reported in the January 18 letter may be symptomatic of systemic failings within the Service and the Department of Justice. The Direction requires that specific candour-related statements, including a declaration, where accurate, that information relied on in an application had not been obtained as the result of any activity that raised a real concern of illegality be included by affiants in supporting affidavits. The Direction also required the addition of specific recitals relating to the duty of candour in all draft warrants placed before the Court.

[29] In April 2019, the Senior General Counsel for the NSLAG wrote to the Court in response to the Direction. He confirmed the Service's intent to comply with the spirit of the Direction but expressed concerns with the wording of the candour-related statements. He proposed to file amendments for the Court's consideration. He also advised that a practice direction would issue to NSLAG counsel addressing the Chief Justice's concerns. In April 2019, that practice direction was provided to the Court. It stated, in part:

> Warrant applications will not rely on information derived from unlawful activity of the Service or its sources. Where unlawful activity occurs it must be brought to the Court's attention in warrant applications so that the Court may fully assess any circumstances which might reasonably be expected to have a bearing on the Court's discretion to issue the warrant. Where there may be doubt as to whether any activity undertaken is lawful, that activity should be drawn to the Court's attention.

[30] In September 2019, the Senior General Counsel for the NSLAG issued a second practice direction addressing the disclosure of information regarding human sources in warrant applications.

[31] Recently, after further direction from the Chief Justice, submissions and proposed amendments addressing the expressed concerns of the Service with the prescribed wording in the Chief Justice's Direction were filed. The direction and its implementation remain before the Chief Justice and nothing in this judgement overtakes or reverses the Chief Justice's Direction or the questions arising from it that are now being considered with the benefit of submissions from *amicus curiae* appointed by the Chief Justice.

G. *Common issues hearings*

[32] The initial application in [Case A] has resulted in protracted proceedings before the Court. The evidence in each of the three applications [Case C] [Case B] and [Case D] and in [Case A] formed part of the record in the common issues proceedings. As the hearings unfolded, additional evidence of potential relevance was identified. The result was the production of documentation, the filing of additional affidavit evidence and the scheduling of additional witnesses as the proceedings unfolded. This included the filing of additional affidavit evidence and the hearing of witnesses after oral submissions were received in June 2019.

[33] In [Case B] and the common issues proceedings a total of 14 affiants placed evidence before the Court. These included senior officials within the Service and the Department of Justice, current and former. A number of affiants have filed multiple supplementary affidavits. Of the 14 affiants, 11 appeared before the Court for examination and cross examination by the *amici*. Each of the required affiants appeared upon request, no subpoenas were issued. Three affiants sought and were granted limited standing in the hearings which included the right to make limited written submissions. In each instance written submissions were provided.

[34] The Court presided over case management hearings and sat to hear evidence or receive oral submissions on 24 days. The final oral hearing took place on November 1, 2019 and the final written submissions were filed with the Registry on November 28, 2019. A further affidavit was filed by the Service on March 23, 2020 providing the Court with a copy of a recently

completed review undertaken to address the use of human source information in [Case D]. I briefly address this report in my concluding remarks.

[35] A summary of the proceedings in [Case B] and in the common issues proceeding, including a listing of affiants identified by position, the dates affidavits were filed and the dates the Court sat are set out in Annex A Appendices 1 through 4 for ease of reference. Annex A Appendices 5 and 6 lists the more significant legal opinions over which privilege was waived and identifies Security Intelligence Review Committee [SIRC] Reports relevant to the issues.

III. Background

A. *How did the issue of illegality arise?*

(1) The Service must act within the law

[36] The Service's mandate under the *CSIS Act* is to investigate threats to the security of Canada (s. 12(1)). This includes the threat of terrorism posed by individuals or groups who are prepared to threaten or use violence for political, religious or ideological reasons (para. (c) of the definition of "threats to the security of Canada" at s. 2). The successful fulfillment of the Service's counter-terrorism mandate is challenging and the consequences of failure are significant. In pursuing its mandate, the Service must identify and obtain access to those who may pose a threat to Canada's security. To do so, the Service uses a variety of tools. Despite the importance of the Service's national security function, the tools available to it are not unlimited.

[37] The Service is limited by what the *amici* have aptly described as its "foundational commitment" to collect intelligence within the bounds of the law. This commitment is rooted in the 1981 McDonald Commission Report, a report that was instrumental in the development of the *CSIS Act*. It reads:

> [21] […] [T]he rule of law must be observed in all security operations. Several meanings have been given to this phrase. The meaning which we have in mind is that expressed by the English writer, A.V. Dicey, when he wrote that
>
> > […] every man, whatever be his rank or condition, is subject to the ordinary law of the realm and amenable to the jurisdiction of the ordinary tribunals […]. With us every official, from the Prime Minister down to a constable or a collector of taxes, is under the same responsibility for every act done without legal justification as any other citizen.
>
> In our context this means that policemen and members of a security service, as well as the government officials and ministers who authorize their activities, are not above the law. Members of the security organization must not be permitted to break the law in the name of national security. If those responsible for security believe that the law does not give them enough power to protect security effectively, they must try to persuade the law-makers, Parliament and the provincial legislatures, to change the law. They must not take the law into their own hands. This is a requirement of a liberal society. It is, therefore, unacceptable to adopt the view, which we have found expressed within the RCMP, that when the interests of national security are in conflict with the freedom of the individual, the balance to be struck is not for the court of law but for the executive. […]
>
> (Canada, Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, Second Report: Freedom and Security Under the Law, vol. 1, Part II, (Ottawa: Privy Council Office, 1981) [McDonald Commission Report] at pg. 45, para. 21. (Also see vol. 2, Part VI, at pg.737, para. 135.) [Emphasis added; footnotes omitted]

[38] Various provisions of the *CSIS Act* are consistent with the McDonald Commission Report's view that "the rule of law must be observed in all security operations" (ss. 12.1(3.4), 20, 21). The jurisprudence also affirms the Service's obligation to uphold the rule of law. In *X (Re)*, 2018 FC 738, Justice Noël wrote that "the *CSIS Act* must be interpreted cautiously to ensure minimal infringement of our most fundamental liberties, while ensuring that the rule of law is upheld" (paras. 22–26; also see *X (Re)*, 2016 FC 1105 [*Associated Data*] at paras. 129–132).

[39] The Minister may issue written directions, commonly referred to as Ministerial Directions, to the Director of the Service regarding the control and management of the Service (*CSIS Act*, ss. 6(1)–6(2)). The Minister has exercised this authority in the form of a Direction relating to the conduct of Service operations and accountability (Ministerial Directions For Operations and Accountability, approved by the Minister of Public Safety and Emergency Preparedness on July 31, 2015, replacing the 2008 Ministerial Direction on Operations and the 2001 Ministerial Direction on Responsibility and Accountability [2015 Ministerial Direction]). The 2015 Ministerial Direction identifies observance of the rule of law as the lodestar in guiding the conduct of Service operations. The 2015 Ministerial Direction states:

> The Government and the people of Canada expect a high level of performance by the Canadian Security Intelligence Service (the Service) in discharging its responsibilities under the *Canadian Security Intelligence Services Act (CSIS Act)*. <u>It is also expected that the Service will perform its duties and functions with due regard to the rule of law and respect for the rights and freedoms guaranteed under the *Canadian Charter of Rights and Freedoms*.</u>

> Pursuant to subsection 6(2) of the *CSIS Act*, I have issued the following direction to describe my expectations in relation to the conduct of the operations by the Service.
>
> **FUNDAMENTAL PRINCIPLES**
>
> The following fundamental principles will guide all Service operations:
>
> - The rule of law must be observed[.] [Emphasis added.]

[40] Thus, the McDonald Commission Report, the *CSIS Act*, the jurisprudence, and the 2015 Ministerial Direction all compel the Service to operate according to law.

(2) The Crown immunity doctrine

[41] The gathering of intelligence in furtherance of the investigation of terrorist threats to Canada presents significant operational challenges. Not surprisingly observance of the rule of law, particularly where the law evolves or changes may, at times, exacerbate the already challenging circumstances in which the Service and its leadership must operate. This occurred in the aftermath of the 2001 terrorist attacks in the United States.

[42] Following those attacks, Parliament passed the *Anti-terrorism Act*, SC 2001 c. 41 [*Anti-terrorism Act*]. The *Anti-terrorism Act* expanded the scope of terrorism offences under the *Criminal Code*. (Part II.1 of the *Criminal Code* is reproduced at Annex B to these reasons for reference.) Among other things, it criminalized the provision of "property or financial services or other related services" for the purpose of benefiting any person facilitating or carrying out any

terrorist activity or knowing that doing so would benefit a terrorist group (*Criminal Code*, s. 83.03). This posed a difficulty for the Service in that gaining access to the subjects of national security terrorism investigation at times requires the provision of money or property to these individuals. The *Anti-terrorism Act* amendments did not exempt the Service from the expanded terrorism provisions. Neither did the *CSIS Act* as it existed in 2001.

[43] This raised the possibility of criminal liability attaching to certain of the Service's activities. Relying on the Crown immunity doctrine, the Service, on the AGC's advice, concluded that criminal liability did not arise in these circumstances.

[44] The Crown immunity doctrine creates a presumption that the Crown is not bound by statute unless the statute expressly states that it binds the Crown; the statute clearly intends to bind the Crown; or the statute would be frustrated, or an absurdity would result, if it did not bind the Crown (*Alberta Government Telephones v (Canada) Canadian Radio-television and Telecommunications Commission*, [1989] 2 SCR 225 at pg. 281). This principle is reflected in section 17 of the *Interpretation Act*, RSC, 1985 c. I-21. Thus, in the Service's view, it was in a position to conduct activities in carrying out its mandate that on their face contravened the *Criminal Code* on the basis that Crown immunity shielded Service employees and human sources from criminal liability and therefore allowed it to operate within the law.

(3) The evolution of legal advice

[45] The Crown immunity doctrine had been a topic of longstanding discussion and concern between the Service and the Department of Justice. This discussion initially took place in light of the Supreme Court of Canada's decision in *R v Campbell and Shirose,* 1999 1 SCR 565 [*Campbell and Shirose*] which addressed the doctrine of Crown immunity in the law enforcement context. There, the Supreme Court held that police officers posing as drug sellers and offering to sell drugs to senior members of a drug trafficking ring had broken the law and did not benefit from Crown immunity. In response, Parliament created a statutory regime through which police officers could obtain pre-authorization to commit otherwise illegal acts in furtherance of a valid law enforcement objective (*Criminal Code,* s. 25.1). This regime does not extend to CSIS, its employees or its human sources.

[46] In April 2002, after the passage of the *Anti-terrorism Act*, the Department of Justice generated an opinion addressing whether the Crown was bound by the amendments to the *Criminal Code*. This opinion relied on the Crown immunity doctrine in expressing the general view that the *Criminal Code* provisions passed under the *Anti-terrorism Act* do not bind the Crown. The opinion noted that the case relied on to support this opinion—*Canadian Broadcasting Corp v (Attorney General) Ontario,* [1959] SCR 188—is dated, and that "it is not entirely clear that the Supreme Court would arrive at the same decision today if a case were to raise squarely the issue."

[47] In 2004, the Service requested advice from its Department of Justice Legal Services Unit (now the NSLAG and referred to throughout as the NSLAG) on the potential liability of human sources and their handlers who may engage in activities which on their face contravene the *Criminal Code*'s anti-terrorism provisions. The NSLAG concluded that Crown immunity shields the Service's human sources and their handlers from criminal responsibility. This opinion relied on the 2002 opinion. It also reiterated the caveats contained in that opinion, cautioning that Crown immunity should not be seen as a panacea for potentially illegal actions in furtherance of the Service's mandate. It suggested legislative reform be considered to resolve the uncertainty.

[48] In an April 2005 email exchange between NSLAG counsel and senior Service officials, counsel provided advice to the same effect, characterizing it as the Department of Justice's "official position." NSLAG counsel went on to express the view that the 2002 opinion is weak, citing a lack of academic and recent judicial support for the Crown immunity doctrine.

[49] The former Senior General Counsel for the NSLAG gave evidence to the effect that the issue arose throughout her nine year tenure, between 2009 and 2018. In early-2011, she initiated work within the NSLAG to generate a discussion paper on the topic. By April 2013, this work culminated in another legal opinion. This opinion concluded that the likelihood of the Service successfully relying on Crown immunity was low and recommended a legislative solution. The opinion highlighted that the Ministerial Direction then in effect required that "the rule of law must be observed" and that human sources were to carry out tasks on behalf of the Service

"without engaging in illegal activities." The opinion concluded that these factors would make it difficult to carry out illegal acts required to achieve mandated objectives.

[50] In September 2013, the Senior General Counsel for the NSLAG placed the 2013 opinion before a meeting of the Service's Litigation Committee. On review of the opinion, the Committee decided to explore the possibility of requesting an amendment to the Ministerial Direction to reflect the availability of Crown immunity and to document proposed legislative changes to ensure the Service was in a position to proceed with legislative reform if given the opportunity. It appears, as noted later in these reasons, that an amendment to the Ministerial Direction reflecting the availability of Crown immunity was pursued in 2015 without success.

[51] In its 2014 – 2015 Annual Report, SIRC—charged with ensuring that CSIS used its powers legally and appropriately—raised concerns with human source operations potentially breaching the *United Nations Al Qaida and Taliban Regulations*, SOR/99-444. It recommended internal mechanisms to ensure that no human source operations violated these regulations or any similar Canadian statute or regulations. This was not the first SIRC study to address the issue of the Service and its human sources potentially engaging in criminal activities. In a report released in 2009 the Committee specifically considered the implications of the anti-terrorism provisions of the *Criminal Code*, noting that "[…] activities considered illegal under the *Anti-Terrorism Act* [are] potentially controversial […] and should be subject to a high level of accountability" (SIRC Review 2008-04 Review of a Human Source Operation). Nor, as described below, was the

2014 – 2015 SIRC Annual Report the last word from SIRC on this issue. The relevant SIRC studies are listed at Appendix 6 of Annex A.

[52] It is worth noting that in conducting its work SIRC had, and its successor the National Security Intelligence Review Agency has, access to any information under the control of the Service. This includes access to all information subject to any privilege under the law of evidence including solicitor-client privilege (*National Security and Intelligence Review Agency Act*, SC 2019, c 13 at ss. 9–12).

[53] In May 2016, following an in-depth review of the Service's foreign fighter strategy and human source operations (SIRC Review 2015-09 CSIS's Investigation of Canadian "Foreign Fighters" [Foreign Fighter Review]), SIRC recommended that the Service seek clarification on whether Crown immunity afforded CSIS employees and human sources protection from the *Criminal Code*'s anti-terrorism offences. In this recommendation, SIRC quotes from what has been described as a preliminary NSLAG opinion addressing the issue of Crown immunity in the context of the specific operation under review. That opinion described the Service's ability to rely on Crown immunity as "a grey area." SIRC was also provided with the 2013 opinion. The above recommendation was repeated in SIRC's 2015 – 2016 Annual Report.

[54] The updated 2015 Ministerial Direction was issued to the Service by the Minister in July 2015. In the course of preparing this update, the Service sought the inclusion of language that would recognize a Crown immunity exception to the requirement that the Service and its

human sources comply with the law. In June 2015, the Department of Justice's Assistant Deputy Minister of Public Safety, Defence and Immigration addressed the request for the inclusion of wording recognizing an exception, stating that the Service likely did not benefit from Crown immunity:

> Justice is unable to provide such wording as the Department has advised that there is a low likelihood that human sources will be able to rely on Crown immunity as a defence in relation to activities that are offences under the *Criminal Code* or other statutes. Moreover, Justice has also advised that there is a low likelihood that CSIS itself (including its officials and employees) would benefit from Crown immunity with respect to such activities. Bestowing of Crown immunity on CSIS is not consistent with the *CSIS Act*, which explicitly addresses unlawful activities, by for example, requiring under ss. 20(2) that the Director report to the Minister, where he is of the opinion that a CSIS employee may have acted unlawfully in the purported performance of his duties.
>
> […]
>
> The new threat diminishment provisions [in the *CSIS Act*] further support this view […]. The *CSIS Act* now refutes any possible argument that activities contravening Canadian law can legitimately be contemplated as "effecting" Crown purposes whether they are carried out by sources or by CSIS officials or employees. [Emphasis added.]

[55] The then Senior General Counsel for the NSLAG describes this opinion as significant because it marks the first time that the Department of Justice unequivocally told the Service that it likely did not benefit from Crown immunity.

[56] It is worth noting that the Service and the NSLAG did not provide SIRC with the June 2015 opinion as SIRC was preparing its Foreign Fighter Review. Nor did the Service or the

NSLAG provide SIRC the June 2015 opinion in response to the recommendation that the Service clarify the availability of the Crown immunity doctrine. This despite SIRC's access to legal advice, the opinion being directly relevant to the review, contradictory of the previous advice that was provided, and seemingly fully responsive to the recommendation that the Service seek legal clarification on the protection afforded by the doctrine.

[57] In October 2015, the NSLAG prepared further written advice for the Service on the issue of Crown immunity. This advice contradicted the Assistant Deputy Minister of Public Safety, Defence and Immigration's unequivocal opinion from June 2015. NSLAG counsel advised in October 2015 that the Department of Justice maintains that the Service "may rely" on Crown immunity, with the caveats relating to the uncertainty surrounding the applicability of the doctrine and the "medium to low chance" of success should the matter be reviewed by a court. The Senior General Counsel for the NSLAG reviewed the October 2015 opinion, felt it was too favourable to the Crown immunity doctrine, and understood that the opinion had not been finalized. However, the advice was delivered to the Service's Deputy Director Operations.

[58] The SIRC recommendation led the NSLAG to prepare a new legal opinion. This new opinion, delivered to the Director of the Service in January 2017, concluded that the Service did not benefit from Crown immunity. The Director recognized that the opinion foreclosed the Service's reliance on Crown immunity and that this would have a significant impact on Service operations. The Director sought a meeting with the Deputy Minister of Public Safety and

Emergency Preparedness, the Deputy Minister of Justice, and the National Security and Intelligence Advisor to discuss the opinion and potential legislative solutions.

[59] In the meeting, the Deputy Minister of Justice advised that senior members of the Department of Justice would review the opinion. The Department of Justice would then advise the Director of the Service and the Deputy Minister of Public Safety and Emergency Preparedness of the result of its review and whether viable solutions short of legislative reform existed.

[60] The Director of the Service understood that the Department of Justice's review would result in a definitive opinion on Crown immunity within a relatively short period. Pending receipt of that opinion, the Director understood that Crown immunity remained the basis upon which the Service could undertake operations that on their face breached the *Criminal Code*. At this point, the Director ceased approving such operations.

[61] The Department of Justice did not deliver a further opinion to the Service in the weeks or months that followed. It never did. It is not clear what inquiries the Director or others made to determine the status of the opinion. Any such inquiries were limited and informal.

[62] The evidence does establish that following the high level meeting at the end of January 2017, the Department of Justice prepared a draft legal opinion for the Deputy Minister as the Director understood would be done. The draft opinion expressed the same conclusion as that

reached in the 2017 opinion: the Service did not benefit from Crown immunity. The Department of Justice did not finalize this draft or deliver it to the Director of the Service.

[63] NSLAG counsel continued to provide legal advice to the Service that addressed the question of Crown immunity in the context of specific human source operations. This advice was provided in compliance with the Service's obligation under the 2015 Ministerial Direction to conduct operational risk assessments. This advice was not responsive to the Service's and more specifically the Director's expectation that a further Department of Justice opinion was to be provided on the issue of Crown immunity.

[64] In the absence of such further advice, the Service continued to conduct previously approved high legal risk operations. Having ceased the approval of new operations following the receipt of the January 2017 opinion, approvals recommenced in late-March 2017. These were operations that the opinion had concluded were illegal.

B. *Service processes*

[65] The evidence identified two processes as being of particular relevance in the context of the candour breach: the assessment of the legal risk of proposed operations and the warrant application process.

(1) Assessing the legal risk of operations

[66] The 2015 Ministerial Direction requires that the Service, in undertaking operations, assess operational risk, political risk, foreign policy risk and legal risk.

[67] The Department of Justice's legal risk assessment framework forms the basis for this mandated legal risk assessment. The framework involves an assessment of risk based on the likelihood and impact of an adverse outcome. It considers these two factors concurrently to assess whether the overall legal risk level is low, medium, or high. The legal risk assessment framework does not capture the concept of illegality. However, it does reflect the theoretical possibility that the likelihood of an adverse outcome is 100%. The Assistant Deputy Minister of Public Safety, Defence and Immigration addressed this on cross examination:

> MR. GOURLAY:
>
> Q. So is it your understanding that the effect of the [January 2017] opinion was to take it from a 4 to a 5 in respect of Crown immunity?
>
> A. Yes. In terms of -- yes.
>
> Q. And if it's a 5, when it's very high legal risk, a 5, is that something that -- let me put it this way. Does the client need to be told, "You can't do it," at that point?
>
> A. Normally, maybe stepping back to the level 4, even with a level 4 or a high legal risk, it would be anticipated that the client in those circumstances would take actions to mitigate the risks, to lower the risk. And my understanding is that CSIS did take actions to mitigate the risk, not completely ceasing their operations, but starting to review their operations.

> Then, when you get to the higher level, normally clients are saying, "No authority, you can't continue."
>
> JUSTICE BROWN: Sorry. Normally the client would...?
>
> THE WITNESS: At the highest level, I would say normally the client, when you say "high risk," takes actions to mitigate risk, and I understand that CSIS in this case did take measures to look at their operations and try to mitigate some of the risk.
>
> JUSTICE BROWN: And at level 5, you said what?
>
> THE WITNESS: Well, level 5, usually there is a certainty that it is unlawful, a degree of certainty.
>
> MR. GOURLAY:
>
> Q. So that's risk that couldn't realistically be mitigated. Is that fair?
>
> A. Sure.
>
> […]
>
> Q. But you are advising them on the legal risk, and you've said that a very high legal risk, a level 5, is risk that cannot be mitigated. Right?
>
> A. Generally speaking, yes.
>
> Q. And where there is virtually no chance of an argument succeeding that the act in question was legal.
>
> A. Right, no credible argument left.
>
> Q. So, in those circumstances, wouldn't you expect the client operating under the rule of law not to go ahead with an operation where that level of risk applied?
>
> A. Yes. Generally, yes. [Emphasis added.]

[68] NSLAG counsel applied this legal risk assessment framework in reviewing human source operations relevant to the warrant application in [Case B] In each case, the legal risk

assessment identifies the issue of illegality and concludes that the Service or individuals acting under Service direction are very probably engaging in illegal activity. The opinions conclude that, short of not pursuing the activity, mitigation options do not exist. One of the opinions notes that that the reliability or value of the information to be collected "does not affect the legal analysis."

[69] Despite the absence of legal authority to conduct the activity, the bottom line legal assessment in each case is that the activities constitute a "high legal risk." In each instance, the Director of the Service approved the proposed operations. Approval was provided on the basis of a weighing analysis where it was concluded the anticipated reliability or value of the information to be gleaned from the operation justified the high legal risk. In one instance, the Director's assessment included reference to a senior official's note to the effect that approval "could be perceived by the Court as ignoring" Justice Noël's concerns in [Case A] Approval was nonetheless granted.

[70] Senior Service officials and the Director balanced the absence of legal authority, characterized as risk, against the anticipated benefits of the operation. In doing so the Service viewed the absence of a legal authority to undertake the operations as being no different than an operational, political, or foreign policy risk. Having approved operations that were on their face illegal, the Service then collected information which in turn was put before this Court in support of warrant applications, without notifying the Court of the likely illegality.

(2) The warrant application process

[71] Before the Service brings an application for a warrant, it subjects the proposed application to an internal review and approval process. Counsel, the affiants, senior Service officials, and senior Department of Justice officials all participate in this process. In conducting this internal review in [redacted] [Case C] [Case A] and [redacted] [Case D] all those involved in this process overlooked the fact that the applications included information gathered through activity that was on its face illegal. An overview of the internal review process will assist in understanding the significance of this failure.

[72] The Deputy Director Operations Secretariat manages the warrant application process within the Service. When the Service decides to apply for a warrant, it identifies an affiant, counsel, and others to prepare and review the application.

[73] Counsel undertake an initial assessment of the information to be relied on in the application to determine if there are sufficient facts to support the issuance of the warrant under section 21 of the *CSIS Act*. A meeting is then held and a schedule is established addressing all of the steps required to prepare the application.

[74] Service analysts then prepare affidavits with the affiant's direct input. Counsel reviews and provides advice on the drafts. At this stage, counsel focuses on ensuring that the affidavits state how and when the information being relied on was acquired.

[75] If human sources are being relied on this will be reflected in the affidavit, but counsel will have no information regarding either the source or the source's relationship to the Service. This information is not provided to counsel at this stage. Instead, counsel is later given the opportunity to review such information, but not to independently access the human source file.

[76] Once a draft affidavit is complete, it is reviewed for factual accuracy and then approval is obtained from the Director General of the Service's Operations Branch seeking the warrant. The Service then sends the affidavit to the NSLAG for further review and preparation for presentation to the Warrant Review Committee. The Director of the Service chairs the Warrant Review Committee. The Senior General Counsel of the NSLAG, the Deputy Director Operations, the Assistant Director Operations, the Assistant Director Collection, the Director General of the Operations Branch seeking the warrant, and a senior representative from the Department of Public Safety and Emergency Preparedness Canada sit on the Warrant Review Committee. The affiant, analyst, and counsel responsible for the warrant application also attend the Warrant Review Committee meeting.

[77] In addition to the draft affidavit, the Warrant Review Committee also has access to a list of foreign agencies and human sources relied on in the affidavit's preparation. Any human source is identified by code name. Limited information relating to the source's reliability, relationship with the Service, and access to the target of the warrant is also provided to the Warrant Review Committee.

[78] After the Warrant Review Committee has reviewed the affidavit, draft warrants are prepared and reviewed. The Deputy Director Operations Review Committee conducts a further review of the facts as set out in the affidavit and ensures that the Warrant Review Committee's comments have been addressed. At the same time, Service analysts generate a "source précis" with the help of the Human Source Operations Section for each human source relied on in the affidavit. The source précis should detail a source's relationship with subjects of the investigations and all other information that is pertinent to an assessment of the source's reliability [redacted] Counsel then review the draft précis, again without the benefit of access to the underlying human source files. The précis is then the subject of a challenge session by the affiant, analysts, counsel and a Human Source Operations Section representative. [redacted]

[79] All section 12 warrant applications are subject to a final review by Independent Counsel from the National Security Group of the Department of Justice. This review is intended to independently verify that the information placed before the Court accurately reflects the content of service records, has been placed in its proper context and its reliability has been accurately portrayed. The Independent Counsel is provided access to all underlying reporting relied upon in the affidavit and the source précis.

[80] Once this process is complete, the Service may file an application.

C. *Bill C-59: Legislative reform to address illegality*

[81] The Service and the Department of Justice had identified the development and implementation of a justification regime as the best means of addressing the issue of illegality. This option, which was consistent with legal advice provided over many years, was provided to the Minister of Public Safety in early-2017. The Service and the Department of Justice then worked to implement this option. When Bill C-59 was tabled on June 20, 2017, it included a justification regime (Bill C-59, *An Act respecting national security matters*, 1st Sess., 42nd Parl., 2017, cl 100 and 101 (first reading June 20, 2017)). The regime came into force on July 25, 2019 (S.I./2019-71, (2019) Canadian Gazette, P. II, Vol. 153, No. 15).

IV. Issues

[82] The issues to be addressed were initially identified in the December 2018 direction. At that time it was recognized that these issues were subject to change as matters progressed. In written submissions the issues have been reformulated and I have characterized them as follows:

A. How did the candour breach occur and how is it to be addressed?

B. May the Court consider and rely on information that was likely collected in contravention of the law?

C. If the Court may consider and rely on information that was likely collected in contravention of the law, then what factors are to be considered and weighed?

D. If, after a warrant has issued, the Court becomes aware that information placed before it was likely collected in contravention of the law, may the Court invalidate the warrant or take other action?

E. Should the Court invalidate an issued warrant, what authority does the Court have to make remedial orders regarding information collected under that warrant? How should the Court exercise that authority?

F. Where information is excised from the application, may the Court continue to rely on the pre-application consultations and approval requirements at subsections 7(2) and 21(1) of the *CSIS Act*?

G. Application to [Case B]

V. Analysis

A. *How did the candour breach occur and how is it to be addressed?*

(1) The duty of candour

[83] Justice Mosley, in *X (Re)*, 2013 FC 1275 [*X (Re)* 2013], aff'd 2014 FCA 249 [*X (Re)* 2014], identified the broad nature and scope of the duty of candour in the context of a warrant application under section 21 of the *CSIS Act*:

[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 (CanLII), [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 (CanLII) at para. 117, rev'd on other grounds 2010 FCA 122 (CanLII), appeal on reserve before the Supreme Court; *Charkaoui (Re)*, 2004 FCA 421 (CanLII) at paras. 153, 154; *Almrei (Re)*, 2009 FC 1263 (CanLII), 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.

[…]

[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, <u>including all facts from which inferences may be drawn</u>. 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 or probable grounds of 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.

> [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. […]
>
> [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. […] [Emphasis added.]

[84] The decision in *X (Re)* 2013, is not the most recent judgment from this Court dealing with candour. SIRC's 2014 – 2015 Annual Report published in late-January 2016, referenced a Service program involving the collection and retention of certain meta or associated data, a program that had been ongoing since 2006 but never disclosed to the Court. The disclosure of this program lead to an *en banc* hearing on June 10, 2016, where the Deputy Minister of Justice and the Director appeared to address the issue of transparency, an issue described by the Chief Justice as going "to the core of the Service's relationship with the Court." This is the candour issue addressed by Justice Noël in *Associated Data.*

[85] In advance of the finding in *Associated Data* that the duty of candour had again been breached and in the course of the June 2016 *en banc* hearing, the Department of Justice advised the Court that Mr. Murray Segal had been retained to advise on best practices in *ex parte* proceedings. Mr. Segal's final report was completed in December 2016 and contained a number of recommendations (Review of CSIS Warrant Practice, Report of Murray D. Segal, December 2016 [Segal Report]).

[86] The Segal Report identifies a series of instances involving candour breaches including, but not limited to, the circumstances addressed by Justice Mosley in *X (Re)* 2013 and Justice Noël's findings in *Associated Data.* The Segal Report explains that the Service and the Department of Justice must do much more than avoid untruth to comply with the duty of candour, and that the duty is not exhausted simply through the inclusion of all relevant information in an application.

[87] The Segal Report also notes that unlike *ex parte* proceedings in other contexts, where full disclosure is generally provided to the opposing party at some later point in the process, this rarely occurs when the Service is applying for a warrant under the *CSIS Act*. Recognizing the unique nature of the national security proceedings, Mr. Segal states that "in no other context is counsel's compliance with the duty of candour more critical to upholding the rule of law."

[88] The Segal Report then addresses Crown counsel's special responsibilities and how they inform the duty of candour when applying for a warrant under the *CSIS Act*:

> Finally the special roles and responsibilities of Crown counsel need to inform how the duty of candour is calibrated in this context. It cannot be forgotten that where counsel representing CSIS comes before the Federal Court seeking a warrant, he or she is representing the Attorney General of Canada. Special duties attach to the Crown that do not burden other parties. As the Supreme Court has stated [in *Ontario v Criminal Lawyers' Association of Ontario*, 2013 SCC 43 at para. 37, per Karakatsanis J.]:
>
> > The Attorney General is not an ordinary party. This special character manifests itself in the role of Crown attorneys, who as agents of the Attorney General, have broader responsibilities to the court and to the accused, as local ministers of justice (see *Boucher v The Queen*, [1995 S.C.R. 16, at pp. 23–24, *per* Rand J.; *Nelles v Ontario*, [1989] 2 S.C.R. 170, at pp. 191–92, *per* Lamer J.).
>
> The Attorney General has unique, overriding obligations to the administration of justice that are deeply rooted in our constitutional traditions. The Federal Court of Appeal [in *Cosgrove v Canadian Judicial Council*, 2007 FCA 103 at para. 51] has neatly captured this idea in speaking of the "traditional constitutional role of attorneys general as guardians of the public interest in the administration of justice (pgs. 14 and 15). [Footnote[s] omitted]

[89] The obligations and responsibilities flowing from the duty of candour are not limited to individuals who appear before the Court. Those who hold leadership positions within the Service and the Department of Justice also have obligations and responsibilities to the Court. Senior managers and leaders are responsible for ensuring those who seek warrants on behalf of the Service recognize the Service's privileged position before the Court. These individuals must do more than recognize the duty of candour's importance: they must identify and implement the institutional structures and processes necessary to ensure individual and institutional compliance with the duty.

[90] Designated judges—as the gatekeepers charged with striking the appropriate balance between private interests and Canada's security needs—have to engage in this balancing exercise without the benefit of the ordinary adversarial process (*Associated Data* at para. 100). As such, designated judges have no choice but to rely on compliance with the duty of candour. To do so, designated judges must possess a high level of trust and confidence that individuals appearing before the Court have fulfilled their obligations. Designated judges must also have trust and confidence that institutional structures, processes and culture have provided the tools and instilled the values necessary to deliver compliance with the duty of candour. While the burden is heavy, meeting it is critical to upholding the rule of law (Segal Report at pg. 14).

(2) The breach of the duty of candour

[91] The AGC has acknowledged that the duty of candour has been breached. However, it submits that counsel and the Service acted in good faith and tried to uphold the duty in this matter and in the applications that were brought before Justice Kane and Justice Brown. The AGC submits that individual conduct is not in issue. Rather, the breach resulted from institutional failures that prevented Service employees and counsel from recognizing the issue of illegality and raising it with the Court.

[92] This explanation does not lessen the corrosive effect of the breach on the Court's confidence in the Service's ability to be candid, a point that was made in the June 2016 *en banc*. Instead, it suggests that the Court cannot rely on the individuals appearing before it to be candid—not because of individual failings, but because of institutional failings that render it

difficult, or perhaps impossible, for individuals to inform themselves of relevant information or to act on the information that they are aware of. This is perhaps more troubling than a single individual's failure to comply with the duty of candour.

[93] There is no doubt that the Service breached the duty of candour in the course of seeking warrants in this matter: whether the Service illegally collected information used to support a warrant application is highly relevant both to the Court's assessment of that information and to the ultimate exercise of the Court's discretion.

[94] Justice Noël, in considering the [Case A] application, was clearly concerned with the nature of the operation that resulted in the collection of some of the information relied on. He initially framed his concern as relating to the Service's authority to undertake the operation in issue; but he also noted payments made to an individual involved in terrorism, and explicitly mentioned the *Criminal Code*. AGC counsel assured Justice Noël that the Service had addressed the issue. This was not the case.

[95] Original counsel in [Case A] was replaced in May 2018. In late-May 2018, new counsel acknowledged before Justice Noël that illegality was an issue. That acknowledgement did not paint a full and candid picture of the history of the issue.

[96] I immediately attribute the failure to accurately respond to Justice Noël's concerns to counsel. However, I also understand that this failure must be placed in its broader, more

concerning context. Service advisors had known for years that the Service was gathering information used for warrant applications through activities that were on their face illegal: senior AGC counsel addressed the issue in 2015; SIRC raised it in 2016; the NSLAG raised it in its opinion in 2017; and throughout this period, the NSLAG provided opinions on the issue of illegality in operational reviews. Despite all this, experienced NSLAG counsel was apparently unaware that illegality was an issue in April 2018. This demonstrates not only a lack of individual awareness but also a severe institutional failing.

(3) The causes of the breach of the duty of candour

[97] The significance of the candour breach in this instance, particularly in light of the history of Service noncompliance with the duty, underscores the necessity of attempting to understand the cause of this breach—not to assign blame, but to assure the Court that the Service and the Department of Justice are taking steps to prevent future breaches. The Service and the Department of Justice must identify and address the causes of the breach to re-establish the Court's trust in their ability to comply with the duty of candour when seeking warrants.

[98] In an effort to understand the causes of the breach, the common issues hearings pursued what AGC counsel has described, somewhat critically, as a searching inquiry. The Court's inquiries were—and needed to be—searching. This Court and the Canadian public deserve to understand how an issue as fundamental as the illegality of CSIS conduct was not identified and disclosed in the warrant application process.

[99] The AGC submits, and I essentially agree, that the evidence shows that individuals within the Service and the Department of Justice made some efforts to equip those involved in the warrant application process with an understanding of the duty of candour after receipt of the Segal Report. The evidence of the individual witnesses also demonstrates that those witnesses possess an understanding of the nature and import of the duty, and that institutional measures have been adopted to meaningfully implement the recommendations from the Segal Report. Despite all this, the Service and counsel for the AGC have acknowledged that the application in [Case A] was deficient and the Court has once again been placed in the position of having to address a serious candour breach.

[100] Institutional failings contributed to the breach. In many instances, it appears that questionable individual decision-making contributed to or exacerbated the impact of these failings. However, and as was noted in the June 2016 *en banc* hearing, for individuals to comply with the duty of candour institutional systems must be designed and implemented in a manner that ensures those who appear before this Court possess all the information they need to satisfy the duty. If institutional systems do not deliver on this core requirement, then the individual commitment to the duty of candour is of limited value, and breaches of the duty will continue to occur.

[101] These reasons focus on institutional shortcomings. This focus reflects the evidence heard and the Court's interest in ensuring that the duty of candour is rigorously upheld on a going-forward basis. The purpose of the common issues hearings was not to inquire into individual

conduct or attribute individual responsibility. However, the fact that these reasons do not review the individual decisions and actions that underpinned the Service having embarked upon operations that have now been acknowledged as unlawful does not negate the fact that the evidence does raise questions with respect to individual decision-making. Individual conduct may well deserve scrutiny, but that scrutiny should occur in another forum.

[102] For this reason I have purposely avoided the identification of individuals by name in these reasons.

[103] Before I address specific institutional failures, it will be helpful to review the steps taken after the delivery of the January 2017 opinion to the then Director of the Service. The events illustrate certain of the institutional failures to be discussed below. They also reveal the Service's troubling willingness to undertake operations in the face of advice to the effect that the *CSIS Act* did not authorize the operation. The events also reveal the Department of Justice's equally-troubling reluctance to clearly and unequivocally communicate that certain proposed operational activity was illegal, and that the Service lacked the authority to undertake the activity.

(4) Events following the January 2017 opinion

[104] After the January 2017 meeting involving the Director, the Deputy Minister of Public Safety and Emergency Preparedness, the Deputy Minister of Justice, and the National Security and Intelligence Advisor, the Department of Justice quickly initiated a review of the January 2017 opinion. In February 2017, a draft opinion was prepared for the Deputy Minister's

signature. This opinion reached the same conclusion as the January 2017 opinion: the Service did not benefit from Crown immunity and legislative reform was needed. This draft opinion was never finalized or sent to the Service. The further work done at the then Deputy Minister's direction identified that law reform was the only option to address the issue of illegality and efforts were then focused on that option, not the generation of another opinion. This conclusion appears to have been reached by mid-February 2017, and by late-February 2017 at the latest.

[105] The Director of the Service expected, but did not receive, a further opinion. The evidence is imprecise on what steps the Director or other Service officials took to determine the status of that opinion but no formal inquiries were made. Similarly, there was no formal communication from the Department of Justice to the Service advising that the opinion was not forthcoming or, in the absence of a further opinion, a communication clarifying the status of the January 2017 opinion. This despite the Director having been advised in writing by the NSLAG Senior General Counsel after the high level January 2017 meeting that "the [opinion] will be reviewed in light of the findings and conclusions that will be reached in this additional work. You may want to retain this note with the earlier memorandum for your records."

[106] The then Director continued to expect a further opinion on Crown immunity up until he retired in May 2017. In the interim, the then Director also understood the Service was to rely on Crown immunity in undertaking any otherwise unlawful operational activity, as it had since 2004.

[107] On receipt of the January 2017 opinion, the Director had ceased approving "high legal risk" operations. In late-March 2017, in the absence of further advice, the Director resumed the approval of such operations where, in the Director's view, the value of the operation justified the risk. The Director's decision to resume the approval of operations where legality was an issue was made without providing any notice to the Deputy Minister of Justice or any other senior officials. As stated by the *amici*, it appears the Service was willing to let sleeping dogs lie.

[108] The Department of Justice also appeared content with the status quo. No formal advice was provided after the high level January 2017 meeting. The Department of Justice's efforts relating to the issue of illegality focused on the development of what appears to be forward-looking legislative reform. The NSLAG continued to legally review Service operations in accordance with the Department of Justice legal risk assessment framework and the requirements of the 2015 Ministerial Direction.

[109] In the absence of the promised further legal opinion, the Department of Justice's position on Crown immunity was less than clear. NSLAG counsel was nonetheless expected to continue to deliver operational legal advice on this issue. Operational legal advisors should not have been placed in this position. Despite being left to their own devices, the operational legal risk assessments that were in evidence indicate that the NSLAG counsel viewed Crown immunity as being unavailable to the Service. Those risk assessments generally concluded that proposed activity that was contrary to Part II.1 of the *Criminal Code*, was not authorized by the *CSIS Act*, and very probably illegal. Nonetheless, and possibly due to the absence of clarity from senior

management, the overarching legal assessment provided by NSLAG counsel to the Service in these instances did not characterize these operations as illegal, but as presenting a "high legal risk."

[110] Senior Service officials, up to and including the Director, relied upon the legal issue being characterized as presenting a high risk in recommending and approving the operational activity. Characterizing illegality as a legal risk in effect permitted the Service to engage in the balancing exercise described above: the Service weighed the benefits of the operations against the risk arising from the illegality. This included a consideration of mitigating options that focused on reducing the gravity of the criminal activity. Reduced gravity of course does not necessarily render an illegal activity legal. It does not impact on the fundamental issue of illegality.

[111] In any event, the result of this balancing analysis was the recommendation and ultimate approval of many operations that the Service's legal advisors considered to be illegal.

[112] After March 2017, it does not appear that any effort was made to address the issue of ongoing illegality by the Service or the Department of Justice beyond the operational legal risk assessment process. Affiants instead described efforts to develop an apparently forward-looking justification regime that was included as part of Bill C-59 upon its introduction in Parliament in June 2017. That legislation received Royal Assent in June 2019. The justification regime and its development do not appear to address the Service's day-to-day activities at the relevant times.

It was not suggested in either written or oral submissions that the justification regime provides any retroactive or retrospective solution to past circumstances of illegality.

[113] The Service's "high risk legal" operations continued. In May 2017, the Director retired. The position was filled on an interim basis by the then Deputy Director Operations pending the arrival of the newly-appointed Director in June 2017. Although the interim Director and incoming Director both knew that Crown immunity was a live issue, both believed that the Department of Justice maintained the position that the doctrine continued to provide some legal protection to the Service in undertaking activities that were on their face illegal.

[114] In September 2017, the Director wrote to the Minister of Public Safety and Emergency Preparedness with a copy of the correspondence to the Deputy Minister of Justice, the Deputy Minister of Public Security, and the National Security and Intelligence Advisor addressing the Service's approach to the management of issues addressed in Bill C-59 pending passage of the legislation. In addressing Crown immunity, he wrote:

> Historically, CSIS has relied on *Crown Immunity* for its authority to conduct operational activities, including human source operations, that involve otherwise unlawful acts or omissions. As you know, Bill C-59 would provide CSIS with explicit legislative authority to undertake these activities.
>
> Pending passage of the Bill, CSIS will continue to rely on its historic interpretation of *Crown Immunity* to conduct such operational activities. In doing so, it will continue to assess the operational, political, foreign policy, and legal risks of activities that would otherwise constitute offences, with the Department of Justice providing legal risk assessments. As with the other three risk pillars, where an elevated risk is determined, the value of the

> operation is measured against identified risks, and opportunities to mitigate such risks are considered. Of note, comprehensive risk assessment training has been developed and will be delivered to CSIS intelligence officers in the coming months.
>
> CSIS continues to conduct thorough reviews of its human source inventory to identify operations of elevated legal risk; this is an ongoing effort. Further to my predecessor's undertakings, I will immediately notify you of high risk operations I approve, should any be identified. [Emphasis added.]

[115] The Director's unambiguous statement that "pending passage of the Bill, CSIS will continue to rely on its historic interpretation of Crown Immunity to conduct such operational activities" is directly at odds with the Department of Justice's conclusion following the January 2017 meeting. Despite this, there is no indication in the record that the Department of Justice made any effort to advise the Director that its most recent work on Crown immunity indicated that it was not available to the Service.

[116] Between June 18, 2017 and January 2019, when the Interim Direction issued ceasing the approval of all potentially illegal operations pending implementation of the Bill C-59 justification regime, the Director approved [> 1 0] potentially illegal activities. In approving these activities or operations, the Director's evidence was that he was unaware of the January 2017 opinion. He did not learn of the opinion until late-December 2018. This was after he had sought legal advice on the issue of Crown immunity in response to the questions of illegality being raised in [Case B]

[117] Service officials and NSLAG counsel were aware of the illegality issue through 2017 and 2018. NSLAG counsel continued to review operations where illegality was the issue and the Service continued to approve the operations after engaging in a balancing analysis. Despite the visibility of the issue, neither senior Service officials nor their legal advisors recognized that the collection of information through these operations would or could impact upon the use of that information in the warrant application process. This despite the Senior General Counsel of the NSLAG having flagged this issue in an email in the fall of 2016.

[118] The proceedings in [Case B] resulted in the Director requesting further advice on the availability of Crown immunity from the then recently appointed Senior General Counsel of the NSLAG in November 2018. That opinion was provided to the Director in January 2019.

[119] The January 2019 opinion reached the same conclusion as that reached in the June 2015 opinion provided by the Assistant Deputy Minister of Public Safety, Defence and Immigration, the January 2017 opinion delivered to the then Director, and the draft opinion prepared for but never delivered by the Deputy Minister of Justice in February 2017. The conclusion was stated as follows:

> It is our legal opinion that there is no lawful basis for the Service to commit criminal offences under the existing legal framework. The *CSIS Act* does not authorise the Service to engage in criminal conduct, even if it yields valuable intelligence.

[120] The Service immediately initiated concrete measures to address the January 2019 opinion: the Interim Direction was issued; active warrants were reviewed to identify instances

where information collected illegally had been relied on in seeking warrants; and the Minister of Public Safety and Emergency Preparedness, the Deputy Minister of Public Safety and Emergency Preparedness, the Deputy Minister of Justice, the National Security and Intelligence Advisor, SIRC, and the National Security and Intelligence Committee of Parliamentarians were briefed.

[121] Almost four years after having been first advised that Crown immunity was unavailable, the Service responded to that advice: operations that in the considered view of the Service's legal advisors were likely illegal would no longer be approved.

[122] It is difficult to overstate how disturbing these circumstances are. Operational activity was undertaken in the face of legal advice to the effect that the activity was not authorized by the *CSIS Act*. Reliance was placed on the Crown immunity doctrine despite the Service having been advised by senior counsel in the context of a revision to the Ministerial Direction that "[b]estowing of Crown immunity on CSIS is not consistent with the *CSIS Act*." Nonetheless, the Service continued to rely on Crown immunity, doing so in the face of unambiguous direction from the Minister of Public Safety and Emergency Preparedness that the "Service must observe the rule of law in discharging its responsibilities." And this was done with the apparent acquiescence of the Department of Justice. While the evidence discloses that the operational activity in issue was reported, in some instances belatedly, to the Minister, the reporting was couched in the language of "high legal risk"—not illegality.

[123] The circumstances raise fundamental questions relating to respect for the rule of law, the oversight of security intelligence activities, and the actions of individual decision-makers. These questions are well beyond the scope of this current proceeding, but are certainly relevant. Observance of the rule of law in not only words but also in fact must be the guiding principle underpinning operational decision-making, even where inconvenient or difficult. If it is not, then how can any Court have confidence that the duty of candour will be respected in difficult or embarrassing circumstances? To paraphrase the McDonald Commission Report, security interests cannot justify the breaking of the law—instead, where the law is overly restrictive, those responsible for security must persuade Parliament to change it (McDonald Commission Report at vol. 1, pg. 45, para. 21). Legislated change has been effected in this instance but that change appears to be forward-looking and does not alter the nature or the character of the illegality that preceded it.

[124] It is also important to note that the "risk" assumed in the approval of these operations included the risk of individual Service employees and Service human sources being subjected to criminal prosecution. Were impacted Service employees and human sources made aware that they were at "high risk" of violating provisions of the *Criminal Code*? If not, then what authority, moral or legal, did the Director and senior Service management rely upon in assuming this risk on their behalf? Similar questions arise in regards to the position of Department of Justice counsel who were required to provide operational legal advice to the Service, in the absence of a clear Department of Justice position on the issue of Crown immunity.

(5) Institutional and systemic issues contributing to the candour breach

[125] The evidence discloses a number of institutional failures that contributed to the candour breach. However, the Court's understanding of the factors contributing the breach is limited by the evidence that was placed before it. Despite the searching nature of the inquiry, the Court has not been exposed to all processes that may be relevant to the candour breach. The identified areas of concern are therefore not exhaustive. They are a starting point for what must, in my opinion, be a more comprehensive review of the processes within the Service and the Department of Justice that impact on the duty of candour. In effect, and despite the expected substantive changes that were to follow the 2016 *en banc* and the Segal Report, serious institutional shortcomings impacting upon the duty of candour remain within the Service and the Department of Justice.

(a) *NSLAG knowledge management and information sharing*

[126] The Department of Justice's position on Crown immunity and Service illegality lacked clarity and was inconsistently understood by counsel and the Service. I highlight three examples:

A. The 2016 SIRC recommendation that the Service seek clarification on the issue of Crown immunity addressed an issue that had been clarified in legal advice provided to the Service and the Department of Public Safety and Emergency Preparedness in 2015. The June 2015 advice appears to directly address the 2016 SIRC recommendation, and was generated by the Assistant Deputy Minister responsible for managing the legal services provided to the Service by the NSLAG. SIRC was not advised of the June 2015

advice in the course of its review. It also does not appear either the Service or the AGC brought this advice to the attention of SIRC as a response to the recommendation.

B. In October 2015, the NSLAG provided the Deputy Director Operations an opinion on the issue of Crown immunity. That opinion makes no reference to the Assistant Deputy Minister's advice a few months earlier. Instead, it states that the official Department of Justice position was that the "Service may rely on Crown immunity." The Senior General Counsel maintained this opinion had never been finalized. However, the Deputy Director Operations received the opinion and understood from it that the Service could continue to rely on Crown immunity.

C. In April 2018, counsel appearing in [Case A] was unaware of legal advice relevant to the file, and in fact appears to have been unaware of the broader issue of illegality in the context of the anti-terrorism provisions of the *Criminal Code*. This despite the numerous pieces of NSLAG advice generated on the issue. This might be attributed to an individual failure however to do so too easily dismisses the institutional responsibility of ensuring that mechanisms are in place to effectively provide those appearing before this Court with the information needed to satisfy the duty of candour.

[127] Knowledge management and information sharing within the NSLAG must be effective and encompass all counsel, particularly those appearing before the Court.

(b) *The Department of Justice legal risk assessment framework*

[128] As noted, the assessment of legal risk arising from Service operations is conducted under the Department of Justice legal risk assessment framework. There was no suggestion in the evidence that the framework was misapplied. Rather, the evidence indicates that it is poorly suited to assessing and addressing potentially illegal activity.

[129] The framework characterizes all issues in terms of risk. This approach at least suggests that the risk can either be accepted or mitigated. Thus, an activity that plainly breaches the *CSIS Act* is characterized as a "high legal risk": one that, when viewed from an operational perspective may be balanced against the benefits of the operation and accepted where the benefits are viewed as being significant. This is exactly what occurred. However, an activity that breaches the *CSIS Act* is not like any other risk. It is activity that on its face is illegal and if undertaken would also be contrary to the Service's foundational commitment to collect intelligence within the bounds of the law.

[130] If the proposed Service activity is not authorized by the *CSIS Act*, there is no room to balance interests: the activity is illegal and cannot proceed, at least not within the bounds of the law. Characterizing unlawful activity in terms of risk does not change the fact that it is illegal.

[131] The legal risk assessment framework mischaracterized Service activity that was on its face illegal as posing a "high legal risk." In doing so, it allowed decision-makers to authorize illegal activity on the basis that it could be weighed against expected benefits. This circumstance not only resulted in the Service engaging in illegal operational activity: it may have also

contributed to the failure of those involved in the warrant approval process to identify the information collected as a result of this activity as having been unlawfully collected. Lack of awareness of illegality has been advanced as one explanation for the breach of candour.

(c) *The interplay between counsel's duty of candour and duty of loyalty*

[132] The *amici* argue that the candour breach continued even after counsel identified illegality as an issue in [Case A] This is because counsel did not candidly advise the Court that the Service was aware, based on the legal advice it had received, of the illegal character of the collection activities it had undertaken. The *amici* argue that counsel was required to seek a waiver of privilege prior to appearing before the Court to allow these circumstances to be fully disclosed.

[133] Counsel provided evidence in this proceeding. She acknowledges that she was mindful of her obligations to not disclose legal advice provided to the Service. However, she also testified that in her view there was no obligation to disclose the Service's degree of knowledge or the legal conclusion reached within the NSLAG at that point in the proceedings. She was of the view that having identified the issue of legality as being one of the legal issues to be adjudicated, and in the absence of an admission of illegality, the legal conclusion reached in the AGC advice was subject to argument and to be decided by the Court.

[134] I am persuaded by the *amici* view: in these unique circumstances candour required that counsel seek a waiver of privilege prior to appearing before the Court. However, I recognize that

counsel was faced with the difficult task of balancing the duty of candour against the duty to protect privilege. This highlights how the duty of candour can conflict with other professional obligations and the rights of the Service. How counsel resolves these conflicts requires active consideration and discussion in advance of a situation such as the one that arose. Neither the Service nor the Department of Justice were well-positioned to identify and engage in a principled balancing of the competing interests early on in the process. This needs to be addressed moving forward.

(d) *The role of the Department of Justice*

[135] Similarly, the Department of Justice's role in circumstances where a client is engaging in activity that it views as illegal requires consideration.

[136] Senior Department of Justice counsel provided evidence in the common issues hearing to the effect that where a client—in this case the Service—is advised that there was no credible basis to conclude a certain activity could legally be undertaken, it was expected that the client would not proceed with that activity. However, counsel was also clear that the Department of Justice's role is not to tell a client what to do.

[137] This may be strictly accurate. Legal advisors are not decision-makers. However, the absence of a decision-making role must be considered within the context of counsel's role as the Attorney General of Canada's representative and the *ex parte, in camera* nature of the proceeding.

[138] Subsection 4(a) of the *Department of Justice Act*, RSC, 1985, c. J-2 imposes an obligation on Department of Justice counsel to do more than simply deliver advice:

***Department of Justice Act*, RSC, 1985, c. J-2**	***Loi sur le ministère de la Justice*, LRC (1985), ch. J 2**
Powers, duties and functions of Minister	**Attributions**
4 The Minister is the official legal adviser of the Governor General and the legal member of the Queen's Privy Council for Canada and shall **(a)** see that the administration of public affairs is in accordance with law[.]	**4** Le ministre est le conseiller juridique officiel du gouverneur général et le jurisconsulte du Conseil privé de Sa Majesté pour le Canada; en outre, il : **a)** veille au respect de la loi dans l'administration des affaires publiques[.]

[139] The Supreme Court of Canada has also held that the Attorney General and his agents are not ordinary parties. They have broader responsibilities in relation to the administration of justice (*Ontario v Criminal Lawyers' Association of Ontario*, 2013 SCC 43 at para. 37).

[140] In his article "Loyalty, Legality and Public Sector Lawyers," 2019 97-1 *Canadian Bar Review* 129 sessional professor and former Chief Legislative Counsel in the Department of Justice, John Mark Keyes examined the duty of loyalty that public sector lawyers owe their client and how considerations of legality limit the duty. In reviewing the rationale for and basic elements of the duty of loyalty, Keyes relies on paragraph 12 of *R v Neil*, 2002 SCC 70 in stating that the duty is essential to preserving the repute of the administration of justice (pg. 132) and

that client confidence in respect for the duty is central to a lawyer's role in the administration of justice (pg. 132, citing *Canada (Attorney General) v Federation of Law Societies of Canada*, 2015 SCC 7 at para. 83).

[141] Keyes notes, however, that the duty of loyalty does not mean that a government sector lawyer is to be silent in the face of illegality. He points to the Federation of Law Societies of Canada's *Model Code of Professional Conduct* as recognizing and reflecting the limits of the duty of loyalty in such circumstances. He concludes that "like other members of legal professional bodies, public sector lawyers are required to withdraw from participating in activities they 'know' constitute wrongdoing" (pg. 137). The threshold is high and is not satisfied where there exists a "risk" of illegality but the limits of the duty of loyalty are reached where "there is no basis for believing there is a legal argument to support government action" (pg. 149).

[142] Keyes further concludes that public sector lawyers do not exercise decision-making power and as such do not attract a higher duty than do other members of the legal profession to advance the values of the rule of law and legality of government activity. While I am not prepared to endorse this view, Keyes does note at page 141 that:

> A public sector lawyer's duty to advance the rule of law is to provide solid advice on the legality of government action […] it is to encourage decisions that not only minimize risk that the action may be challenged legally and found to be outside the law, but also advance constitutional values, including the rule of law.

[143] What is "solid advice"? Keyes does not define the term but it must as a minimum capture the concepts of coordinated, timely and unambiguous advice, advice that is developed and delivered to encourage the decision-maker to undertake actions that are consistent with the rule of law.

[144] In the face of activity involving the administration of public affairs that is inconsistent with the rule of law, it cannot be enough to simply provide legal advice and let the chips fall where they may. As discussed above, in September 2017, the Director gave the Department of Justice formal notice that the Service, as a matter of policy, "will continue to rely […] on *Crown Immunity*" to conduct unlawful operational activities. The Department of Justice's apparent inaction in the face of this information where it had reached the conclusions set out in the January 2017 opinion fall well short of its obligations to ensure that public affairs are administered according to law.

[145] In this regard, I note that the McDonald Commission Report recognized the importance of the role of the Minister of Justice in ensuring a security intelligence agency operates within the law, stating that the Department of Justice's role is crucial in ensuring that "[…] the security intelligence agency conducts its activities within the law" (McDonald Commission Report, vol. 2, Part VIII, at pg. 878, para. 84).

[146] The McDonald Commission Report also addresses the role of the legal advisor where an issue of illegality arises, stating:

> [136] […] The advice of the legal adviser as to the legality of an operation must be binding on the agency unless a contrary opinion is given by the Deputy Attorney General of Canada. Any knowledge by the legal adviser, either before or after the fact, of any illegal act by the agency must be reported by him to the Deputy Attorney General of Canada (McDonald Commission Report, vol. 2, Part VI, at pg. 737–738, para. 136).

[147] This is not to excuse the Service. It shares responsibility for what, in its best light, can be characterized as an unwillingness to clarify legal advice impacting on the lawfulness of its operations.

(e) *The warrant application process*

[148] The warrant application process generally involves a detailed, multi-step process. Despite this, no one involved in it recognized the illegality issue, or that inclusion of information in the warrant applications collected through "operations not authorized by the *CSIS Act*" must be disclosed to the Court in order to comply with the duty of candour.

[149] How the issue was not identified is far from clear. Many individuals involved in the review and approval process were at least aware of the issue of illegality subsequent to the January 2017 opinion. They had also participated in the review and approval of the operations involving illegality and relied on in the warrant applications.

[150] Further, in the fall of 2016, in two separate documents, NSLAG counsel identified to the Service that reliance on illegally collected information could impact on how that information

may be treated by a designated judge. The NSLAG addressed the issue as follows in draft advice that was provided to the Service:

> "Finally, the Service should consider flagging reporting from REDAC in a particular way so that it can monitor closely whether information obtained from REDAC is used in making applications for warrants pursuant to s. 21, or for making disclosure to law enforcement pursuant to s. 19. This is because the information being relied on or disclosed will be up for examination by a court and, in the context where it is relied on by law enforcement to support eventual criminal charges, subject to challenge by an accused. In terms of consequences, relying on information that itself was obtained illegally could engage a whole host of liabilities, including impacting the outcome of criminal prosecutions. Thus care should be exercised in allowing this information to be used in judicial proceedings. [Redactions in original.]

[151] Despite the NSLAG's warning to the Service that a "host of liabilities" could arise from using illegally collected information in other judicial proceedings, the Service carried on with this practice.

(f) *Information silos and compartmentalization*

[152] One reason why the Service and its counsel did not identify illegally collected information as an issue is that information relevant to the warrant application process was inaccessible, or not readily accessible, to those involved in the process. This is particularly the case in regards to human source files.

[153] The November 7, 2019 affidavit filed on behalf of the Service describes a number of measures undertaken to address this issue. Since August 2019, NSLAG counsel involved in the application process have had access to human source files whenever necessary in the application preparation process. The Service also established the CSIS Affiant Unit in August 2019. Finally, the Service has engaged a former Deputy Minister of Justice to review Service practices regarding disclosure of information about human sources in warrant applications. This review is focused on the non-disclosure in [Case D] These measures are all represented as responsive to the issue of affiant and counsel access to human source files.

[154] However, information silos and compartmentalization extend to others that play key challenge and approval roles in the process. The changes described in the November 2019 affidavit do not address how senior individuals, both legal and operational, failed to identify the illegality issue in fulfilling their challenge and approval functions.

[155] The issue of illegality was not new to senior officials in the Service or the NSLAG. The consequences of relying on information from the impugned operations were identified as problematic by NSLAG counsel in late-2016. The Director's evidence was that he approved [>10] of these operations between June 2017 and December 2018. In this context, even if it was not evident that a specific questionable operation was linked to a warrant application, the possibility that this would arise was not hypothetical. Yet no senior individual identified or sought to address this possibility in recommending warrant applications moving forward.

[156] The decision to extend broader access to human source files to application counsel is essential if counsel is to meaningfully fulfill their role. However, this requirement was highlighted to the Service by Justice Noël in *Harkat (Re)*, 2009 FC 1050 (paras. 48–49). The implementation at this point, of a measure that was identified as necessary by a designated judge over a decade ago does little to contribute to the rebuilding of confidence and trust.

(g) *Communications among senior Service officials*

[157] The facts disclosed in the common issues proceedings also raise questions relating to information sharing among senior Service officials.

[158] Remarkably, the evidence indicates that senior operational decision-makers within the Service had little more than a general knowledge of the January 2017 opinion. This despite the fact that the then Director described the opinion as likely requiring the Service to stop a number of counter-terrorism operations and as potentially having enormous implications on Service employees. Although the then Director participated in a senior level meeting outside the Service to address the implications of the opinion it does not appear the opinion was subject to similar scrutiny among and between senior officials within the Service. This absence of a shared and detailed understanding of the opinion extends to the details surrounding the further advice the then Director expected to receive from the Department of Justice.

[159] The absence of any detailed awareness among senior Service officials of an issue that held such enormous implications for the Service is surprising and difficult to comprehend.

How was a legal opinion that in the Director's opinion so fundamentally impacted upon the Service not the subject of detailed review, discussion and analysis at senior levels within the service? This was not explained in the evidence. Similarly the resumption of the approval of high risk operations in March 2017 raises questions relating to knowledge and communications both within and outside the Service.

[160] The approval of operations impacted by the January 2017 opinion was suspended by the then Director after he received the opinion. Following the January 2017 meeting with the Deputy Minister of Justice and others, the Director expected a further legal opinion addressing the ability of the Service to rely on the Crown immunity doctrine. He continued to expect this opinion until his retirement in May 2017. In the absence of this further opinion and without any notice to senior officials outside the Service, most importantly the Deputy Minister of Justice, the Director recommenced the approval of impacted operations in March 2017. In doing so, the first approvals of "high legal risk" operations included a caveat stating the approval was provided pending a final opinion from the Department of Justice. This caveat disappeared from later approvals.

[161] Despite approving a significant number of operations that were characterized as "high legal risk" because they involved illegality, the incoming Director was not aware of the January 2017 opinion. He was aware that an opinion was forthcoming from the Deputy Minister of Justice on Crown immunity. However, neither he nor any other senior official within the Service sought to determine the status of the anticipated opinion. Had such an inquiry been made,

presumably the Director would have been told no further advice was to be provided, a decision that had been reached within the Department of Justice by late-February 2017. Similarly, in seeking the Director's approval of operations involving illegality, no senior official within the Service or the NSLAG advised the Director of the existence of the January 2017 opinion, the final substantive advice the Service had received on the issue of Crown immunity.

[162] The issue of illegality appears to have simply not been a topic of discussion. There was a willingness to rely on the framing of the issue as one of risk to be weighed against other interests and objectives pending receipt of legal advice, advice that was not pursued. Both senior Service officials and the Department of Justice were also content to view legislative reform as the solution. But of course this solution did not address ongoing operational activity or provide a basis upon which to approve operational activity prior to the limited justification regime coming into force.

(6) Conclusion on candour

[163] The security intelligence function is vital to the nation's security. I appreciate the challenges that those charged with the responsibilities of carrying out this function face. Despite these challenges, this Court and the Canadian public must have confidence that respect for the rule of law is and remains a foundational principle underpinning all national security intelligence decision-making. The circumstances disclosed here suggest a degree of institutional disregard for—or, at the very least, a cavalier institutional approach to—the duty of candour and regrettably the rule of law.

[164] This is not to suggest that departures from the rule of law may not, very exceptionally, arise. Error, poor judgment, or perhaps even exigent circumstances may result in a departure from this foundational principle. Section 20 of the *CSIS Act* recognizes this possibility and provides a mechanism for reporting and addressing such circumstances.

[165] In *Associated Data*, Justice Noël queried what must be done to ensure this Court's findings in relation to candour are taken seriously:

> [108] […] I find that the CSIS has breached its duty of candour by not informing the Court of its *Associated Data* retention program. In *X (Re)*, cited above, my colleague Justice Mosley, on a different factual basis, also concluded that a breach of the duty of candour had occurred. I make a similar finding three (3) years later. I wonder what it will take to ensure that such findings are taken seriously. Must a contempt of Court proceeding, with all its related consequences, be necessary in the future? [Emphasis added.]

[166] I am left with the same question.

[167] In 2016, after the Court's June *en banc* and the conclusion in *Associated Data* that the Service had breached the duty of candour, the Service made efforts to improve its ability to comply with the duty. These efforts included the commission of the Segal Report, enhanced reporting to the Court, and improved individual training in respect of candour obligations and the issuance of a joint Service–Department of Justice policy addressing the duty of candour (Policy of the Department of Justice Canada and the Canadian Security Intelligence Service on the Duty of Candour in *ex parte* Proceedings, February 23, 2017). These efforts suggest that the Service

and the Department of Justice did take the Court's conclusions seriously. Yet, even as the Segal Report recommendations were being implemented, the events underpinning this latest candour breach were unfolding.

[168] The evidence indicates that the issue of potential illegality was widely known within the circle of those organizations and institutions that play a role in the oversight or management of CSIS operations. SIRC has undertaken reviews and identified concerns to the Service; Public Safety and the Privy Council Office also had knowledge not later than January 2017 as a result of the meeting convened by the then Director that was attended by the then Deputy Minister of Public Safety and the then National Security Advisor. Despite this widespread knowledge and the potential relevance the issue of illegality had in the context of warrant applications, the matter was never brought to this Court's attention. This is inexcusable, particularly where there was a heightened awareness of the import of the duty of candour and ongoing engagement between the Court, the Service and the Department of Justice in the aftermath of the *Associated Data* decision and the Segal Report. It appears only the Court was left in the dark.

[169] A contempt proceeding may lead to institutional or individual consequences. It would provide a forum for the Court to again express its concerns with the breach and the circumstances underlying it. This might be adequate if the breach were linked to discrete individual or institutional failings. It is not. There are many factors that contributed to this latest candour breach. These reasons have flagged some of those factors. But this is not a complete or comprehensive catalogue of the shortcomings that contributed to the breach. A contempt

proceeding would also fall well short of exploring and addressing the rule of law questions that have arisen in these proceedings.

[170] The breach of candour in this instance is symptomatic of broader, ongoing issues relating to the Service's organizational and governance structure and perhaps institutional culture. The common issues hearings have raised questions relating to the manner in which legal services are structured and delivered to the Service and, even more fundamentally, the roles and responsibilities of AGC counsel. Why were interim measures to address the issue of illegality not pursued prior to January 2019? To not address these questions, questions that impact upon but extend well beyond the matter before the Court, will negatively impact upon public confidence and trust in the Service.

[171] The candour issue arises in the context of illegality. In this regard, Justice Binnie's comments at paragraph 73 of *Campbell and Shirose* are highly relevant:

> […] Police illegality of any description is a serious matter. Police illegality that is planned and approved within the RCMP hierarchy and implemented in defiance of legal advice would, if established, suggest a potential systemic problem concerning police accountability and control. The RCMP position, on the other hand, that the Department of Justice lent its support to an illegal venture, may depending on the circumstances, raise a different but still serious dimension to the abuse of process proceeding.

[172] Service illegality is as serious as police illegality. To not seek out and address the systemic problems that resulted in this breach of candour will negatively impact upon public confidence and trust in the Service.

[173] In addressing the impact of the *Associated Data* decision in the course of his evidence the Director of the Service identified the importance of public confidence and in turn the confidence of the Court in the Service:

> I became Director in 2017 after the Service and the Court had to deal with the [*Associated Data*] decision of Justice Noël. For me it was extremely formative to see the impact that this decision, negative decision for the Service, if I can put it this way, had on the Service and on the confidence of Canadians. It gave me an opportunity to reflect on that. This is why it became one of the two tenets of my early days as Director of CSIS when I issued my message to employees that we needed to maintain and enhance the confidence of Canadians and the Court in our institution.
>
> So, the relationship between the Court and the Service is absolutely fundamental in order for us, CSIS, to discharge our very important mandate on national security. [Emphasis added.]

[174] I share the Director's view. The Service's ability to successfully and effectively fulfill its vital role requires that it have the confidence of Canadians and this Court. As I have previously stated, that confidence has again been shaken. Illegality, or the likelihood thereof, was not proactively disclosed; in fact it was not even identified by the Service or the Department of Justice in the preparation of warrants. The illegality in these instances did not arise in context of exigent or unforeseen circumstances; it arose in the context of a difficult reality. In the face of that difficult reality, consciously or not, the institutional response was to act as though it did not

exist. A contempt proceeding will not re-establish confidence. The circumstances and events that resulted in the Service engaging in illegal conduct contrary to legal advice warrants a comprehensive and detailed review, a review that is mandated to consider broad issues of institutional structure, governance and culture within both the Service and relevant elements of the Department of Justice. Anything less than this will, in my view, fall short of ensuring that confidence and trust in the Service as a key national institution is restored and enhanced.

[175] It is beyond my authority to order this type of comprehensive review. However, this authority does reside within the Executive. I strongly recommend and encourage that the knowledge and expertise available to the Executive within bodies such as the National Security and Intelligence Committee of Parliamentarians, the National Security and Intelligence Review Agency, the Intelligence Commissioner's office, and among outside experts be leveraged for this purpose. A comprehensive review must not only have a mandate to consider the issues identified in this judgment but must seek a full understanding of the underlying events in order to address the systemic, institutional and, if required, individual failures disclosed as a result.

[176] I will now turn to consider the legal questions that have arisen.

B. *May the Court consider and rely on information that was likely collected in contravention of the law?*

[177] The AGC acknowledges that the Service must comply with the law in collecting information in furtherance of its national security mandate. Nonetheless, the AGC submits that

the Court should not automatically exclude illegally obtained information from a warrant application. Instead, it argues that a flexible standard is required, one that involves judicial discretion following a consideration of various factors.

[178] The *amici* do not disagree. However, the *amici* additionally submit that the doctrine of excision found in the section 8 *Charter* jurisprudence is a source of guidance on this issue (*Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c. 11 [*Charter*]; *R v Grant*, [1993] 3 SCR 223 [*Grant #1*]; *R v Araujo*, 2000 SCC 65 [*Araujo*] at para. 57; *R v Mahmood*, 2011 ONCA 693 at para. 116).

[179] The common law recognizes that a judge may exclude evidence where its admission would affect the fairness of the proceeding (*R v Harrer*, [1995] 3 SCR 562 [*Harrer*] at para. 41). In the criminal context, a judge may exclude evidence under subsection 24(1) of the *Charter* not obtained in breach of the *Charter* but that would nonetheless render a proceeding unfair. Exclusion under subsection 24(1) occurs because admission of the evidence would undermine the *Charter*'s guarantee to a fair trial (*Harrer* at para. 42). The exclusion of evidence under either the common law or subsection 24(1) involves a flexible, context-based analysis (*R v Jaser*, 2014 ONSC 6052 [*Jaser*] at para. 28; *R v Wray*, [1971] SCR 272, at pp. 293–296).

[180] Evidence collected in violation of an individual's *Charter* rights is also not subject to automatic exclusion. Rather, under subsection 24(2) of the *Charter*, a judge shall exclude

evidence collected in violation of an individual's *Charter* rights if, having regard to all the circumstances, its admission would bring the administration of justice into disrepute.

[181] The section 8 jurisprudence that the *amici* argues should guide the Court here departs from the flexible, context-based approach to the exclusion of evidence under the common law and subsection 24(1). Under section 8, if misleading, erroneous or unconstitutionally obtained information was relied on in obtaining a warrant, that information is automatically excised. Once the information has been excised, the Court must then consider whether it could have issued the warrant based on the remaining information. However, automatic excision for the purpose of determining warrant validity does not extend to automatic exclusion of information collected under a warrant determined to be invalid.

[182] If the Court concludes on the basis of the information that remains after excision that the warrant was invalid, the Court must then consider whether the admission of the illegally collected information would bring the administration of justice into disrepute in accordance with subsection 24(2). The ultimate evidentiary admission decision engages a contextual consideration of relevant factors in accordance with the subsection 24(2) jurisprudence.

[183] In *Grant #1*, Justice Sopinka notes that the excision doctrine prevents the state from benefiting from the illegal acts of police while allowing warrants that would have otherwise issued to stand:

> [79] […I]n circumstances such as the case at bar where the information contains other facts in addition to those obtained in contravention of the *Charter*, it is necessary for reviewing courts to consider whether the warrant would have been issued had the improperly obtained facts been excised from the information sworn to obtain the warrant: *Garofoli*, *supra*. In this way, the state is prevented from benefiting from the illegal acts of police officers, without being forced to sacrifice search warrants which would have been issued in any event. Accordingly, the warrant and search conducted thereunder in the case at bar will be considered constitutionally sound if the warrant would have issued had the observations gleaned through the unconstitutional perimeter searches been excised from the information. It has been admitted that the police had reasonable grounds for the issuance of a warrant before undertaking either of the perimeter searches. This admission on the part of the respondent is eminently proper given the following independent reasonable grounds identified in the information sworn to obtain the warrant. [Emphasis added.]

[184] As noted by Justice Code in *Jaser* the excision doctrine has survived, but not without two major critiques. First, the rule creates an anomaly: when considering the validity of a warrant, a judge must automatically excise evidence arising from a *Charter* breach or that was otherwise unlawfully obtained, while, at trial, the judge will only exclude that same information following a careful balancing under subsection 24(2) (*Jaser* at para. 26, citing *R v Chau*, [1997] OJ No 6322 at para. 50, aff'd on other grounds 2000 CanLII 17015 (ON CA)). Second, the source of the excision doctrine is not clear: it does not appear to be a subsection 24(1) or 24(2) remedy as it is rigid, categorical, and lacks proportionality; nor does it appear to be a common law remedy as it is not based on any traditional exclusionary principle such as trial fairness, reliability, abuse of process, or the balancing of probative value and prejudicial effect (*Jaser* at para. 28).

[185] The purpose of the excision doctrine—to prevent the state from benefiting from illegal acts of persons acting on its behalf—is relevant in the security intelligence context. However, an automatic exclusion rule in a *CSIS Act* warrant application would attract the same criticisms identified by Justice Code in *Jaser*.

[186] If I were to adopt an automatic excision standard in this instance, illegally collected evidence placed before this Court in the national security context would have to be excised, when that same evidence might well be found admissible in a criminal proceeding under subsection 24(2). An automatic excision rule could lead a designated judge to not issue a warrant due to a minor illegality even where the threat under investigation is significant. Such a stringent test would ignore the role of a designated judge in balancing the societal interest in maintaining national security against individual rights and interests and in turn might well undermine public confidence.

[187] Designated judges considering warrant applications under section 21 are "gatekeepers of intrusive powers, ensuring a balance between private interest and the state's need to intrude on that privacy for the collective good" (*Associated Data* at para. 100). This gatekeeper function must include the authority to weigh competing interests and factors when issues of evidence admissibility arise. This conclusion is consistent with the jurisprudence and is reflective of past practice in designated proceedings.

C. *If the Court may consider and rely on information that was likely collected in contravention of the law, then what factors are to be considered and weighed?*

[188] In the absence of jurisprudence addressing the treatment of illegally collected information in the *CSIS Act* warrant process, the AGC and the *amici* have, as noted above, relied on *Charter* and common law jurisprudence. Although the contexts differ, there is overlap between the interests underpinning a subsection 24(2) analysis and the interests that arise where security officials, in furtherance of a national security investigation, rely on illegally collected information in seeking judicial authorization to intrude on individual rights, including privacy rights protected under section 8 of the *Charter*.

[189] In *R v Grant*, 2009 SCC 32 [*Grant #2*], the Supreme Court considered the test for the exclusion of evidence under subsection 24(2) of the *Charter*. The majority held that the administration of justice "embraces maintaining the rule of law and upholding *Charter* rights in the justice system as a whole" (para. 67). It also held that the phrase to "bring the administration of justice into disrepute" refers to the need to maintain the integrity of and public confidence in the justice system over the long term (para. 68). This involves an objective inquiry that considers whether a reasonable person informed of the relevant circumstances and values would conclude that the admission of evidence would, on a prospective basis, bring long term disrepute to the administration of justice (para. 68). Finally, the Supreme Court held that exclusion of evidence under subsection 24(2) is not driven by punitive or compensatory objectives. Instead, it is driven by a social focus on the broad impact of admitting evidence collected in breach of the *Charter* on the long term repute to the justice system (para. 70).

[190] On the basis of these principles, the Supreme Court found that the issue of repute to the administration of justice engages three inquiries: (1) the seriousness of the infringing state conduct; (2) the impact of the breach on the accused; and (3) society's interest in the adjudication of the case on its merits. The Court's role is to assess and balance each line of inquiry in determining whether, in all the circumstances, admitting the evidence would bring the administration of justice into disrepute (para. 71).

[191] Where the question of evidence exclusion arises in circumstances where there is no alleged *Charter* breach, the jurisprudence recognizes that a judge may exclude evidence relying on either the common law or subsection 24(1). Trial fairness guides the exercise of judicial discretion in such instances. But like the lines of inquiry that are to be considered under subsection 24(2), the trial fairness inquiry involves a consideration of the question of fairness from the perspective of both the accused and the general public (*Harrer* at para. 45).
The common law exclusionary rules involve the consideration of questions relating to trial fairness, abuse of process, and the balancing of the probative value of the evidence against its prejudicial effect.

[192] As is the case in the criminal context, maintenance of the rule of law—including compliance with *Charter* rights and values—are important considerations in the national security law context. This is reflected by Part II of the *CSIS Act*, entitled Judicial Control, and in much of the designated proceedings jurisprudence (*Associated Data* at para. 130; *X (Re)*, 2018 FC 874 at para. 43 and *X (Re)*, 2018 FC 738 at paras. 22, 24 and 66).

[193] In *Grant #2*, the Supreme Court instructs that in considering the seriousness of the conduct in issue and whether consideration or admission of the evidence might be perceived as judicial condonation of the impugned conduct, a court must consider whether the illegal conduct was minor, inadvertent, undertaken in good faith, or in extenuating circumstances. These factors may lessen the need for a court to disassociate itself from the conduct. On the other hand, a court may have to disassociate itself from illegal conduct that is deliberate, negligent, or wilfully blind of the law. Evidence suggesting a pattern of abuse will tend to support exclusion (paras. 74–75). Each of these factors is readily applicable where illegality is in issue in the *CSIS Act* warrant application process.

[194] Similarly, the second line of inquiry requires a consideration of the impact of the breach and whether admission or consideration of the evidence might signal that individual rights are of little consequence. This requires a consideration of the extent to which the conduct undermined protected interests.

[195] Relying on the considerations relevant to the exclusion decision in the contexts outlined above, and having considered submissions of the AGC and the *amici*, I am of the view that this Court should consider three factors when determining whether information connected to illegal conduct should be admitted in support of a warrant application: (1) seriousness of the illegal activity; (2) fairness; and (3) societal interest. Each factor requires a court to consider a series of different questions:

A. *Seriousness of the illegal activity:*

i. Was the illegality minor, technical or trivial, or was it a significant breach of the law?

ii. Did the illegality arise out of inadvertent or unwitting conduct undertaken in good faith, or was it pursued knowingly, out of ignorance, recklessness, negligence, or willful blindness?

iii. Was the illegality isolated or part of a broader pattern of conduct?

B. *Fairness:*

i. How closely linked was the illegal activity to the collection of the information?

ii. Did the illegality meaningfully impact on individual legal rights or interests?

iii. Does the illegality undermine the credibility or reliability of the information?

C. *Societal interest:*

i. Are there extenuating circumstances including, but not limited to, the immediacy or severity of any threat to the security of Canada, linked to the unlawfulness?

ii. Are there any other factors that arise out of the unique circumstances of the case?

[196] As is the case under subsection 24(2), a court should consider these factors and the underlying questions in the context of the overall impact a decision to exclude the impugned information would have on the long-term repute of the administration of justice. There must be a particular focus on the expectation that national security investigations are to be undertaken

within the bounds of the law. The inquiry is objective, asking what a reasonable and informed individual would conclude (*Grant #2* at para. 68).

[197] The factors must be considered collectively. The weight given to each factor will vary based on the circumstances.

D. *If, after a warrant has issued, the Court becomes aware that information placed before it was likely collected in contravention of the law, may the Court invalidate the warrant or take other action?*

(1) A designated judge may review a prior decision to issue a warrant

[198] Although not in issue in the matter before me, the consequences of the Court becoming aware of circumstances or conduct after warrant issuance that could have impacted on the exercise of judicial discretion does arise in the matters before Justice Kane and Justice Brown. In addition the Service has undertaken a review of its files to determine whether the issue of illegality taints other previously issued warrants. This review raises the possibility that other warrant applications considered by this Court have been, or will be, identified as being impacted by conduct that was likely illegal. The authority of the Court in these circumstances was also the subject of written and oral submission in the common issues hearings. In the interests of completeness, I will therefore address the question.

[199] Given the *ex parte* nature of the proceedings, the AGC concedes that it may be appropriate, where a warrant has issued in the absence of full disclosure of illegal activity, that

the Court retains the jurisdiction to address this and consider the warrant's ongoing validity. The AGC acknowledges that a designated judge can rescind a warrant if it should not have been granted in the first place.

[200] The AGC relies on *R v Garofoli*, 1990 CanLII 52 (SCC), 2 SCR 1421 [*Garofoli*] in its submissions on the analysis a judge should conduct in determining whether to rescind a warrant. Under the *Garofoli* framework, where a judge conducts an *ex post facto* review, the judge must ask, after addressing the non-disclosure, if the original warrants could have issued based on the remaining record.

[201] The *amici* also take the position that the Court retains jurisdiction over its warrants and that this allows the Court to act when it becomes aware of illegality relating to a warrant.

[202] I agree with the common position advanced in submissions. The Court has the inherent right to review an *ex parte* order where new facts come to light after its issuance that could have impacted on the exercise of judicial discretion. Preferably, the designated judge who issued the warrant will conduct the *ex post facto* review (*Wilson v the Queen*, [1983] 2 SCR 594 at pgs. 607 and 625).

[203] Justice Mosley exercised this authority in *X (Re)* 2013. He issued a warrant to the Service in January 2009 for a three-month period. He re-issued the warrant in April for a further nine months. He provided written reasons in support of the issuance. In November of 2013,

Justice Mosley issued further reasons in response to recent developments relevant to his January 2009 and April 2009 warrant issuing decision:

> [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.

[204] In issuing further reasons, Justice Mosley does not directly address the question of his authority to review the previously issued warrant well after it had expired. However, it appears the AGC did not object to the Court's authority to do so. His further reasons were appealed. On appeal, it does not appear that the AGC contested the Court's authority to address the issue of non-disclosure after the warrants issued and expired (*X (Re)* 2014).

[205] In *Minister of National Revenue v RBC Life Insurance Co et al*, 2013 FCA 50 [*RBC*], the Federal Court of Appeal considered the Federal Courts' authority when reviewing an *ex parte* application under the *Income Tax Act*, RSC, 1985, c. 1 (5th Supp.). The Court of Appeal noted that judicial discretion is essential to the constitutional validity of an authority that allows for actions comparable to a seizure, even when those authorities arise in a non-criminal context

(*RBC* at para. 23). It then considered the Federal Courts' powers to address a failure to make full and frank disclosure in an *ex parte* proceeding:

> [31] The Minister's submission also raises issues of a more fundamental nature. A breach of the obligation to make full and frank disclosure of information relevant to the Court's exercise of discretion on an *ex parte* application, such as that contemplated under subsection 231.2(3), can hobble the Court's ability to act properly and judicially, and can result in the making of orders that should not have been made. It is an abuse of process.
>
> […]
>
> [33] The Federal Courts have a power, independent of statute, to redress abuses of process, such as the failure to make full and frank disclosure of relevant information on an *ex parte* application: *Indian Manufacturing Ltd. v. Lo et al.* (1997), 1997 CanLII 5346 (FCA), 75 C.P.R. (3d) 338 AT PAGE 342 (F.C.A.); *May & Baker (Canada) Ltd. v. Motor Tanker "Oak"*, 1978 CanLII 2055 (FCA), [1979] 1 F.C. 401 at page 405 (C.A.).
>
> [34] These authorities speak of the Federal Courts' power as being "inherent." At one time, these authorities were perhaps open to the question on the basis that the Federal Courts, as statutory courts, do not have inherent powers. However, this is no longer the case.
>
> [35] The Supreme Court has confirmed the existence of "plenary powers" in the Federal Courts, analogous to the inherent powers of provincial superior courts: *Canada (Human Rights Commission) v. Canadian Liberty Net*, 1998 CanLII 818 (SCC), [1998] 1 S.C.R. 626 at paragraphs 35 to 38 (a case arising in another context, but stating a principle of universal application). These plenary powers are especially live in situations where the Court is exercising its "superintending power over the Minister's actions in administering and enforcing the Act.": *Derakhshani*,supra at paragraphs 10-11.
>
> [36] In my view, <u>the Federal Courts' power to investigate, detect and, if necessary, redress abuses of its own processes is a plenary power that exists outside of any statutory grant, an "immanent attribute" part of its "essential character" as a court</u>,

> just like the provincial superior courts with inherent jurisdiction: see *MacMillan Bloedel Ltd. v. Simpson*, 1995 CanLII 57 (SCC), [1995] 4 S.C.R. 725 at paragraph 30. The Federal Courts' power to control the integrity of its own processes is part of its core function, essential for the due administration of justice, the preservation of the rule of law and the maintenance of a proper balance of power among the legislative, executive and judicial branches of government. Without that power, any court – even a court under section 101 of the *Constitution Act, 1867* – is emasculated, and is not really a court at all. See *MacMillan Bloedel, supra* at paragraphs 30 – 38, citing with approval K. Mason, "The Inherent Jurisdiction of the Court" (1983) 57 A.L.J. 449 at page 449 and I.H. Jacobs, "The Inherent Jurisdiction of the Court" (1970), 23 C.L.P. 23; and see also *Crevier v Quebec (A.G.)*, 1981 CanLII 30 (SCC), [1981] 2 S.C.R. 220. [Emphasis added.]

[206] This reasoning applies equally in the context of warrant applications under the *CSIS Act*. To conclude that the Court lacks authority to review previously issued warrants where issues of candour subsequently come to the Court's attention would insulate the Service from the consequences of its actions. Similarly, the Court would be powerless when faced with information that calls into question whether a warrant would have issued had the Court been provided all relevant information. This would "hobble" a designated judge's ability to act as a gatekeeper of the state's intrusive powers (*RBC* at para. 31; *Associated Data* at para. 100). It would also undermine public confidence in the rule of law.

(2) The *Garofoli* framework, modified to reflect the context, guides the conduct of an *ex post facto* review

[207] In considering the appropriate test to be applied when reviewing a previously-issued *CSIS Act* warrant, it is helpful to consider the jurisprudence addressing the review of criminal search warrants.

[208] Before the police can undertake a search, the *Charter* generally requires that they establish on oath that reasonable and probable grounds exist to justify the search and that evidence will be found at the place of the search (*Hunter v Southam Inc.*, [1984] 2 SCR 145 [*Hunter*] at pg. 168).

[209] Where a criminal search warrant is challenged, the reviewing judge must, after having excised improperly obtained evidence from the information to obtain, assess whether the warrant could have issued without the excised information (*Garofoli* at pg. 1452; *Araujo* at para. 53). The question is not whether the reviewing judge "would" have issued the warrant, but whether sufficient credible and reliable information remains after excision to provide a basis on which the warrant "could have issued" (*R v Morelli*, 2010 SCC 8 at para. 40 [*Morelli*]). If, after excising all impugned facts, sufficient information remains, the warrant will stand.

[210] In determining the question of sufficiency, a reviewing judge may consider additional "amplifying" information that was available at the time of application for the purposes of correcting minor good faith technical errors made in the preparation of the information (*Morelli* at paras. 41–43).

[211] A reviewing judge should not set aside a warrant unless satisfied on the whole of the material presented that there was no basis for the authorization (*Garofoli* at pg. 1454).

[212] In *Araujo*, the Supreme Court, citing the Nova Scotia Court of Appeal's decision in *R v Morris* (1998), 134 CCC (3d) 539 [*Morris*], acknowledges that although deliberate or fraudulent misconduct will not automatically invalidate a warrant, the jurisprudence does not foreclose this result. A reviewing judge may set aside a warrant where the misconduct is so subversive of the process, that it is necessary to do so to protect the pre-authorization process (*Araujo* at para. 54).

[213] In *R v Bacon*, 2010 BCCA 135 [*Bacon*], the British Columbia Court of Appeal affirmed that the role of the review judge was to "strip away objectionable features and examine the sufficiency of what remained" (para. 26). Evidence of fraud, material non-disclosure or misleading information is relevant to the sufficiency inquiry. The British Columbia Court of Appeal did not close the door to a residual discretion to strike down a warrant but held that any such discretion would only arise where an abuse of process had been established (para. 27).

[214] In the civil context, it has been held that even inadvertent non-disclosure can result in the prompt dissolution of an *ex parte* order (*MTS Allstream Inc. v Bell Mobility Inc. et al*, 2008 MBQB 103 at para. 71). On initial consideration, the civil law approach may assist in informing the Court here. However, the issues of misconduct and non-disclosure that arise in

ex parte orders in relation to disputes between private parties engage different considerations than those before me. I have concluded that the civil law jurisprudence is of little assistance here.

[215] The criminal warrant jurisprudence is more applicable to the present situation. Although a *CSIS Act* warrant serves a different purpose than a criminal warrant, I see no reason why the *Garofoli* framework should not apply to the *ex post facto* review of a *CSIS Act* warrant. Like a criminal warrant, a *CSIS Act* warrant authorizes government intrusion into an individual's privacy. The pre-authorization process serves the same purpose in the national security and criminal contexts: the prevention of unjustified searches before they occur (*Hunter* at pg. 160). In both contexts, the state bears the onus of demonstrating that a warrant should issue and that it has met the preconditions for doing so.

[216] In this respect, I note that Justice Edmond Blanchard applied the *Garofoli* framework in reviewing a *CSIS Act* warrant in *Mahjoub (Re)*, 2013 FC 1096. Justice Blanchard was asked to quash warrants issued on the basis of omissions and errors in the information placed before the issuing judge. Relying on *Garofoli*, he concluded that the warrants could have issued (para. 133). The Court of Appeal endorsed this conclusion in *Mahjoub v Canada (Citizenship and Immigration)*, 2017 FCA 157:

> [267] In my view, the different nature of section 21 warrants does not justify a different legal standard. The fact that a section 21 warrant may be hard to challenge in some contexts does not logically lead to the conclusion that when it is challenged in court for omissions or inaccuracies — exactly like a criminal law search warrant — it should be subject to a different legal test. In terms of legal policy, it is hard to understand why a section 21 warrant that

> could have issued despite omissions or inaccuracies should be treated differently from a criminal law warrant. In fact, given the ever-increasing need to guard against terrorism and other threats to national security it is difficult to understand why admissibility standards in the national security context should be more stringent than those in the criminal law context. [Emphasis added.]

[217] In endorsing *Garofoli*'s "could have issued" standard, the Court of Appeal did not consider whether the impugned information should automatically be excised in an *ex post facto* challenge to the warrant.

[218] I have already concluded that excision of illegally collected information in the application process is to be determined on the basis of a contextual analysis that considers and balances the seriousness of the illegality, fairness, and societal interests. The reasons for that conclusion include the need to ensure there is an informed understanding on the part of the designated judge of the circumstances surrounding the illegal conduct, the reliability of the information in issue, and the nature or degree of the threat the state may be exposed to should the information be excluded from consideration. The fact that the same issue arises but in an *ex post facto* review does not change the rationale for engaging in a contextual balancing analysis to determine what information is to be excised in advance of engaging in the required sufficiency inquiry.

[219] The balancing analysis to be undertaken where an issue of illegality is brought before the Court in an *ex post facto* review engages the same factors identified at paragraph 195 above: (1) seriousness of the illegal activity; (2) fairness; and (3) societal interest. Each of these factors would in turn engage a consideration of the previously identified subsidiary questions.

[220] An approach that involves a balancing of factors for the purposes of determining the validity of a national security warrant in the context of a candour breach requires that I depart from *Garofoli* in this respect. The criticisms of the *Garofoli* approach—that it creates an anomaly and that it stands on shaky doctrinal ground—reinforces my decision to do so (*Jaser* at paras. 25–29). In so departing, my conclusions are limited to the circumstances that have arisen in these matters: the determination of validity where a warrant for ongoing national security purposes is called into question for reasons relating to a breach of candour. I am not suggesting that the automatic excision standard would not or should not apply where a national security warrant is challenged in the context of an ongoing criminal proceeding.

[221] Once an excision determination has been made, the designated judge should then apply the "could have issued" standard. In doing so, the judge will consider the information remaining on the record, including any "amplifying" evidence correcting any minor good faith technical errors made in the application, to determine whether the conditions prescribed at subsection 21(3) of the *CSIS Act* could have been met. If they have, the warrant will stand. If not, the warrant must be struck.

[222] *Garofoli*'s "could have issued" standard does not displace the Court's power to redress abuses of its own processes that may arise in instances where non-disclosure involves a breach of candour or some other form of improper conduct on the part of the Service or the AGC (*RBC* at para. 36). This possibility is recognized in the *Garofoli* jurisprudence (*Morris* at pg. 553; *Araujo* at para. 54; *Bacon* at para. 27). In such a circumstance, the Court might consider a number of

remedies, the most significant being the striking of the warrant. However, in my opinion, as in the criminal context, a designated judge should not strike an otherwise valid warrant unless the underlying conduct is particularly egregious.

[223] As a matter of practicality and in furtherance of the efficient use of judicial resources, when faced with the review of a previously issued warrant for reasons of candour, a designated judge may commence with a sufficiency assessment after automatically excluding the impugned information as an initial procedural step. This is essentially the approach adopted by Justice Noël in [Case A] However, if automatic excision leads to the conclusion that the warrant could not have issued then I am of the view that the designated judge would be required to engage in a full balancing analysis prior to reaching a final conclusion on the question of whether the warrant could have issued.

E. *Should the Court invalidate an issued warrant, what authority does the Court have to make remedial orders regarding information collected under that warrant? How should the Court exercise that authority?*

(1) The Court may make orders in respect of the use or retention of information collected under the authority of an invalidated warrant

[224] The AGC takes the position that the Service may maintain information obtained pursuant to an invalidated warrant where the information satisfies the strictly necessary requirement for retention under section 12 of the *CSIS Act* (*Associated Data* at para. 256). Further, the AGC submits that the Court's jurisdiction over information collected pursuant to a *CSIS Act* warrant is unclear and should be approached with caution. It states that the Federal Court—as a statutory

court created under section 101 of the *Constitution Act, 1867*—can only act within its statutory confines (*Constitution Act, 1867* (UK), 30 & 31 Vict., c. 3, reprinted in RSC 1985, Appendix II, No. 5; *Windsor (City) v Canadian Transit Co*, 2016 SCC 54 at para. 33). It acknowledges that the Court has the implied powers necessary to carry out its statutory mandate (*Canada (Human Rights Commission) v Canadian Liberty Net*, [1981] 1 SCR 626 at para. 17) and plenary powers to address abuses to its process (*RBC* at paras. 33 and 36). The AGC also acknowledges, and the jurisprudence confirms, that through its implied and plenary powers this Court has the authority to rescind or vary a warrant (*X (Re)* 2014; *RBC* at para. 33; *CSIS Act*, s. 21(4)(f)). However, this authority, it submits, does not necessarily extend to the issuance of a remedial order impacting the retention or use of information collected pursuant to an invalidated warrant.

[225] The AGC notes the absence of any express provision authorizing the issuance of remedial orders within section 21. It contrasts this with the recently enacted dataset regime within the *CSIS Act* which limits dataset use by the Service in specific circumstances (s. 11.15(5)) and expressly authorizes the Court to take appropriate measures in reviewing the lawfulness of dataset querying and exploitation pursuant to the process prescribed at section 27.1. I do not find this argument persuasive.

[226] The dataset regime is new to the *CSIS Act*. The *CSIS Act* defines a "dataset" as "a collection of information stored as an electronic record and characterized by a common subject matter" (*CSIS Act*, s. 2). Section 11.01 defines three types of datasets: publicly available datasets, Canadian datasets, and foreign datasets. Sections 11.01 to 11.25 prescribe the

collection, retention, use and destruction of datasets. This includes a requirement that datasets containing information predominately relating to individuals within Canada or Canadians be judicially authorized (*CSIS Act*, ss. 11.13–11.15). The *CSIS Act* does not contemplate judicial remedial measures in the context of this judicial authorization process.

[227] The express legislative authority for the Court to take remedial measures that the AGC relies upon arises in a different context: that being a statutorily mandated judicial review to be undertaken where the National Security and Intelligence Review Agency has formed the opinion that the Service's querying and exploitation of a dataset may not have been in compliance with the law (s. 27.1).

[228] This is not analogous to the judicial authorization processes provided for at sections 11.13 and 21. Those processes require the weighing of competing societal and individual interests within a statutory framework. The outcome of that weighing process, while guided by the statutorily prescribed criteria, is within the full discretion of the designated judge. The exercise of that discretion depends upon, among other things, the Service fully complying with its duty of candour. This engages the Court's implied and plenary powers to address abuses directly relevant to the exercise of that discretion.

[229] The jurisprudence—albeit limited and arising in the pre-*Charter* criminal law context—supports the view that this Court's plenary authority includes the discretion to order remedial measures in respect of an invalidated warrant, including destruction of the information collected

pursuant to that warrant (*Bergeron et al v Deschamps et al*, [1978] 1 SCR 243 at pp. 244–245). Within the criminal law context, it has been found that to conclude otherwise would render the quashing of the warrant meaningless (*Re Chapman and the Queen*, 46 OR (2d) 65, [1984] OJ No 3178 (QL)). In the *Charter* era, section 24 reflects the principle that a warrant-issuing court has the discretion, at least in the course of a proceeding, to impose a consequence where information has been obtained illegally or in violation of rights.

[230] The AGC also submits that any consideration of an order for destruction of collected information requires consideration of the Service's retention and disclosure obligations as set out in *Charkaoui v Minister of Citizenship and Immigration and Solicitor General of Canada*, 2008 SCC 38 [*Charkaoui*], where the Supreme Court of Canada held that the Service is bound to retain information it collects that is within the legislatively imposed limits of its activities. The AGC further submits that the consideration of remedial measures must be undertaken recognizing that in setting aside a warrant any collection undertaken pursuant to that warrant is presumptively unreasonable under section 8 of the *Charter* and that this itself is a meaningful remedy. In this instance the AGC also points to the concrete steps it has taken to address systemic and institutional failures in submitting that further remedial action is not required.

[231] I do not disagree. However, these arguments do not impact upon the scope of the Court's remedial authority in the face of an invalidated warrant. Instead, these matters are to be considered in the course of considering whether and how a Court will invoke its discretionary authority to address an abuse of its process resulting in the invalidation of a warrant.

[232] The Court's undisputed authority to rescind or vary a warrant issued on the basis of erroneous information or the failure to make full and frank disclosure includes the authority to take remedial action in respect of information collected under the warrant. To conclude otherwise may well undermine public confidence in the administration of justice.

[233] Remedial measures may include restrictions on the use, the isolation of, or possibly the destruction of the information collected pursuant to the invalidated warrant. What, if any, remedial measures are appropriate is to be determined by the designated judge with the benefit of case-specific submissions that address the circumstances resulting in warrant invalidation and other factors such as the Service's retention and disclosure obligations as set out in *Charkaoui*. The AGC has taken the positon that the three-part analytical framework set out in *Grant #2* would best inform this analysis.

[234] The *Grant #2* framework does engage the issues that would arise in this context. However, it is not necessary that I embark upon a consideration of all of the factors and circumstances to be considered. Suffice it to say that where a warrant is invalidated the Service cannot simply rely on its mandate to argue that information collected under the invalidated warrant will remain fully available to the Service. The AGC must be prepared to address the issue of remedial measures and demonstrate why such measures would not be appropriate.

(2) Retaining jurisdiction over collected information by way of condition

[235] The *amici* submit that in addition to the Court's inherent jurisdiction to order remedial measures, the Court may also rely on its statutory authority to impose "such terms and conditions as the judge considers advisable in the public interest" at the time of issuance (*CSIS Act*, s. 21(4)(f)) to retain jurisdiction over information collected pursuant to a warrant. The *amici* have proposed both a warrant condition and a recital to be used in future warrants independently or together. If adopted, the *amici's* proposed language would set out and confirm the Court's ongoing authority to issue orders relating to the use or retention of information collected pursuant to the warrant where candour issues subsequently arise.

[236] The AGC submits that paragraph 21(4)(f) does not allow the Court to impose terms in a warrant that would provide indefinite control over the information collected pursuant to that warrant. The AGC points to subsection 186(4) of the *Criminal Code* which provides the authority to impose conditions where wiretap activities are judicially authorized. The AGC notes that the term "public interest" in paragraph 186(4)(d) is understood as permitting judicially imposed conditions relating to the execution of the warrant, not the use or retention of information collected pursuant to the warrant (*Lyons v The Queen*, [1984] 2 SCR 633 at pg. 672). The AGC argues that paragraph 21(4)(f) of the *CSIS Act* must be interpreted in the same manner.

[237] The *amici* note in response that subsection 21(4) of the *CSIS Act* is not limited to collection activities but also addresses the retention of incidentally collected information (s. 21(4)(d.1)). The *amici* also submit that *CSIS Act* warrants currently impose limitations on the retention of certain information.

[238] Having concluded that the Court may exercise its inherent authority to address the use or retention of information where it has invalidated a warrant, I need not decide whether paragraph 21(4)(f) provides an independent source of authority in this regard.

[239] In responding to the *amici*'s submissions relating to the inclusion of a recital or condition reflecting the Court's inherent authority in this respect, the AGC is of the view that it would be redundant and not necessary. The *amici* argue that inclusion would have the salutary effect of highlighting the Court's inherent authority.

[240] I am persuaded that the salutary effect of a recital reflecting the Court's inherent authority to make further orders relating to information collected pursuant to the warrant would be of benefit. The *amici* have proposed the following language:

> I have put the Service and the Attorney General on notice that, if it is determined by the Court that the application for this warrant was supported by information that ought not to have been relied on by the Court, or was brought without compliance with the Service's and the Attorney General's duties of candour to the Court, this Court may make orders limiting or prohibiting the use or retention of information collected pursuant to this warrant.

[241] The Court routinely works with templated language when considering warrant applications. However, the language used and conditions imposed in any particular warrant are within the discretion of the issuing judge. The *amici*'s proposed recital has not been exposed to the broader Court through an *en banc* process as was the case in *Associated Data* (paras. 201–252). I am therefore not prepared to order a template change. However, and pending a process

that will allow a broader consideration of the need for and the language of a recital and/or condition, the Service shall ensure designated judges are:

A. notified that the Court's inherent authority will allow it to address non-compliance with the duty of candour subsequently brought to the Court's attention and that this includes the authority to make orders in respect of the use or retention of information collected under a subsequently invalidated warrant; and

B. presented with a proposed recital that reflects the wording set out at paragraph 240 above.

F. *Where information is excised from the application, may the Court continue to rely on the pre-application consultation and approval requirements at subsections 7(2) and 21(1) of the CSIS Act?*

[242] A final issue arose in the course of these proceedings relating to the adequacy of pre-application consultation and approval where information is then excised from an application.

[243] Prior to applying for or seeking renewal of a warrant, the Director of the Service or a designated employee must consult with the Deputy Minister (s. 7(2)) and the Minister must approve of the warrant (s. 21(2)). If consultation and approval has not taken place, the Court cannot grant a *CSIS Act* warrant.

[244] The AGC and the *amici* have addressed whether the Court may continue to rely on a consultation and approval after material information has been severed by the Court, or where

circumstances that may have been material to the consultation and approval, such as illegality, subsequently come to the Court's attention.

[245] The AGC takes the position that subsequent findings by a warrant issuing judge do not nullify the consultation and approval. It submits that the requirement to consult with the Deputy Minister and obtain Ministerial approval prior to seeking a judicial warrant reflects the distinct roles Parliament intended for the Executive and the Court. The Executive's role is to assess the gravity of the threat to national security for the purpose of determining if a warrant should be sought; the Court's role is to assess and weigh the evidence put forward in support of the warrant. The AGC submits that the *CSIS Act* provides the Minister with the tools necessary to ensure that judicial findings are brought to the Minister's attention and provides the Minister with the authority to act in appropriate circumstances, including the authority to direct the Service to cease executing a warrant (s. 6).

[246] The *amici* argue that one must presume the consultation with the Deputy Minister is intended to be meaningful and to include an assessment of the likelihood of the application succeeding. The *amici* submit that where the Court materially alters the record by severing evidence as the result of illegality that was not identified in the course of the consultation, the Court may conclude that the consultation no longer meets this requirement. Similarly, the *amici* submit that one cannot presume that material illegality would not have been relevant to a Minister in considering approval of the application.

[247] The purpose of the Director's obligation to consult the Deputy Minister prior to applying for a warrant is not addressed in the legislation. The McDonald Commission Report does address the role of the Deputy Minister in the warrant application process. The report states that the objective of including the Deputy Minister in the process is to ensure the Minister benefits from the advice of "the most experienced and senior officials of [the] Department" when deciding whether a warrant should be sought (McDonald Commission Report, vol. 1, Part V, pg. 553, para. 95). I therefore agree with the *amici*: the Deputy Minister consultation fulfills a meaningful function. Fulfillment of that function will only occur where the Deputy Minister is made aware of all material facts.

[248] The purpose of Ministerial approval is addressed in the legislative record. Solicitor General Robert Kaplan, appearing before the House of Commons Justice and Legal Affairs Standing Committee, described it as a consideration of "whether the national security is affected or not." Solicitor General Kaplan went on to say that in considering whether to approve of a warrant application, "the Minister assesses the gravity and approves of a warrant if he feels the game is worth the candle." To fulfill this purpose—to decide if "the game is worth the candle"—the Minister needs accurate disclosure of the relevant facts. This would presumably include being advised of questions involving the legality of the collection methods used to obtain the information being relied on to obtain the warrant.

[249] The severance of information or the subsequent disclosure of illegality after completion of the consultation and approval process would be of interest to the Minister and Deputy

Minister involved in that process. However, I am unable to conclude that these circumstances vitiate the prior consultation and approval process. The consultation and approval must be evidenced before the Court acts, but the Court is not informed of what was disclosed to the Deputy Minister or the Minister. What was disclosed may be the subject of privilege. It is not for the Court to guess or surmise the content of the consultation or the factors or circumstances considered by the Deputy Minister or the Minister.

[250] Although the pre-application consultation and approval process prescribed in the *CSIS Act* is not vitiated as a result of circumstances or facts discovered in the course of judicial consideration of a warrant application, a designated judge seized with a warrant application retains a broad discretion in respect of a decision to issue warrants. Where significant information is severed from a warrant, illegality is revealed, or other material circumstances are disclosed it is always open to the designated judge, in the exercise of this broad discretion, to decline to issue a warrant until the Deputy Minister and Minister are notified of those circumstances.

G. *Application to [Case B]*

(1) Overview

[251] As previously described, a decision in [Case B] was initially reserved pending consideration of the underlying legal issues. Due to the pending expiration of warrants issued in [Case A] and the broadening scope of the inquiries arising out of the *en banc* proceeding and

the common issues hearings I received and heard updated evidence in April 2019. The requested warrants were issued. What I referred to as a Supplemental Order formed an integral part of the issued warrants. That Order:

A. details the procedural history as of April 4, 2019;

B. describes the additional affidavit evidence filed in response to prior undertakings and updates the Court on the Service's investigation into the threat related activities of the [redacted] subjects of the warrant application;

C. notes that counsel for the AGC had provided the Court an unsigned copy of the September 6, 2018 affidavit where the information obtained through activities directly linked to the legal issues before the Court was identified, by highlighting, for the Court's benefit;

D. notes that the highlighted information in the unsigned copy of the September 6, 2018 affidavit provided to the Court was excluded from consideration in assessing the application; and

E. notes that information provided by [redacted] human sources was considered, the Court being satisfied this information predated any alleged unlawful activity [redacted] or would otherwise have been available to the Service [redacted]

[252] Although not noted in the Supplemental Order, the information obtained through activities directly linked to the legal issues before the Court was also identified, by highlighting in the April 1, 2019 affidavit. This information was also excluded from consideration in assessing the application.

(2) The Service [investigation]

[253] The September 6, 2018 and April 1, 2019 affidavits set forth information to establish that the [redacted] subjects of the Service investigation identified in [Case A] and [Case B]—[redacted]—are Canadian citizens who had travelled [redacted] remained [redacted] at the time warrants were sought and have participated in fighting with various groups associated with extremist interpretations of Islam. Each is identified as having links to other radicalized individuals who have in turn called for attacks against, or are linked to terrorist attack planning, against Western countries. The affiant expresses the belief that warrants are necessary to investigate the threat posed by these individuals in the event of their return to Canada.

[254] Prior to bringing the initial application in [Case A] the Service had undertaken non-warranted collection activities. These efforts involved the Service initiating and executing what is referred to in [Case B] as the Service [investigation]

[255] The [investigation] led to the collection of information that was relied upon in the [Case A]. In examining the affiant in that application, Justice Noël sought additional detail and

clarification in a number of areas, including the Service's authority to undertake the [investigation] and the propriety of payments the affidavit disclosed had been made

[256] The [investigation] was detailed in the evidence filed in [Case B]. That evidence was to the effect that the investigation of Canadian foreign fighters is particularly challenging. In an effort to collect information on the threat related activities of individuals in hostile and difficult locations the Service [conducted an investigation, during which it paid an individual known to be facilitating or carrying out terrorism an amount totalling less than $25,000 over a few years.]

[257]

[258] [redacted]

[259] [redacted]

(3) Other instances of illegality

[260] In addition to the potential illegality arising from the payments [in the course of the investigation] [redacted], six additional instances of potential illegality were reported to the Court as this matter proceeded. The identified illegality involved the Service or human sources acting on the Service's behalf making payments or providing goods to [redacted]. In one of the six reported instances, a payment that was to be made [redacted] was intentionally interrupted prior to receipt.

[261] Each of these instances is detailed in a chart prepared by counsel for the AGC in the common issues hearings. The entries from that chart that are relevant to this matter are reproduced at Annex C to this judgment and reasons.

(4) Illegality and the exclusion of information

[262] The circumstances in which a designated judge might receive and consider information that was likely unlawfully collected has been one of the focuses of the common issues hearings. My conclusions in respect of these issues have been detailed above. In short I have concluded that where a designated judge is satisfied that information relied upon in a warrant application has been likely unlawfully collected the designated judge might nonetheless consider that information but only after weighing identified factors and circumstances.

[263] At the time I considered and reached a final determination on this application the Service and the Department of Justice had acknowledged the breach of the duty of candour. The Service had also disclosed the circumstances in which payments, goods or services had been provided in contravention or potential contravention of the *Criminal Code*. The information collected through those sources and the [investigation] and relied upon in the application was identified. While I did not at this stage engage in a consideration of whether I was satisfied that the potentially illegal conduct was, on a balance of probabilities, unlawful, I nonetheless opted to exclude all of the impugned information from consideration.

[264] I have since concluded above that automatic excision of unlawfully collected information is an approach that lacks the nuance necessary to assess, consider and weigh the circumstances that might have resulted in unlawful collection in the national security context. A decision to exclude information that is necessary to support a warrant application should, in my view,

involve a consideration and weighing of the factors and circumstances identified earlier in these reasons.

[265] However, prior to engaging in that weighing analysis it is not inappropriate for a designated judge to first ask whether the potentially tainted information is necessary to support the application. If, having excluded the tainted information, sufficient reliable information remains to justify the issuing of the warrants sought, then the judge may decide to proceed on the basis of the remaining information. The exclusion of the information in this initial assessment does not occur because the information is immaterial or irrelevant to determining whether the section 21 criteria have been satisfied (*R v G.B.* (application by Bogiatzis, Christodoulou, Cusato and Churchill), [2003] OJ No 3335, para. 11). Instead, it is an assessment as to whether, within the context of all remaining information, the impugned information is necessary to allow the designated judge to reach a conclusion on the application. Where the impugned information is not necessary the judge need not engage in either a consideration of whether the conduct was illegal or undertake the weighing analysis.

[266] Having adopted an initial exclusion approach in this instance and having been satisfied on the basis of the remaining information that the warrants could issue I need not consider whether I am satisfied, on a balance of probabilities, that the Service activities in issue were unlawful, a matter that is in any event now conceded by counsel for the AGC in all but two of the circumstances identified at Annex C, where either funds or goods were provided. Nor need

I engage in the balancing of interests and the weighing of factors described earlier in these reasons. These issues are essentially moot at this stage in the process.

[267] In issuing the warrants the Court was unaware of one instance of potential illegality, the transfer to [a target] from a human source of [a financial benefit valued at less than $20]. This transfer was approved by the Service and brought to the Court's attention after being identified by the Service in the course of its file review of human sources relied upon in obtaining active warrants after receiving the January 2019 opinion.

[268] This incident of potential illegality involved a source who had also transferred funds to . That transfer had been disclosed prior to the issuance of warrants. Information originating with that source was not excluded from consideration as all information relied upon in the application predated the funds transfer. The source's information also predates the subsequently disclosed transfer. Neither incident of potential illegality impacted upon the information relied upon in the application. The late disclosed transfer would not have impacted upon the decision to issue the warrants.

[269] In concluding that the warrants could issue, I was mindful that the issuance of warrants is a matter that is decidedly within the discretion of the Court; the *CSIS Act* provides that where satisfied the "judge may issue a warrant" (s. 21(3)). A breach of candour and illegality are circumstances that might well militate against issuing warrants even where the requirements for

doing so are otherwise satisfied. However, in this instance I was satisfied that warrants not only could but should issue.

(5) Remaining issues

[270] The issues identified in [Case A] and addressed in [Case B] are broader than the question of actual or potential illegality arising from the [investigation] and other human source activities. I will address each of the remaining matters in turn.

(a) *The Service's authority to undertake the [investigation]*

[271] AGC counsel submits that [investigations of the type in issue] are a technique long relied upon to investigate crime. The technique is available to the Service where the operation is duly authorized, does not infringe a protected right and does not amount to an abuse of process. The *amici* agree with this view.

[272] Section 12 of the *CSIS Act* authorizes the Service to collect information and intelligence. Although the *CSIS Act* does not describe the operational techniques available to the Service in the fulfillment of its section 12 mandate, section 18 of the *CSIS Act* does reference "covert operational activities of the Service" — "des activités opérationnelles cachées du Service."

[273] Service policies address the conduct of [redacted] activity and prescribe the processes for authorizing [redacted] activity. The evidence indicates

that the [investigation] in issue was approved within the Service and that the [investigation] was undertaken to investigate a threat to the security of Canada arising from the activities of Canadian foreign fighters. I am satisfied that the [investigation] was lawful and authorized in accordance with Service procedures.

[274] Similarly there is no suggestion that protected rights were infringed in the process of collecting information during the course of the [investigation] or that the Service engaged in coercive or abusive activity. I am satisfied that the Service had the authority to undertake the [investigation] and that the manner in which the [investigation] was conducted did not infringe on individual rights.

(b) *[Electronic communication]*

[275] In conducting its investigation into the threat posed by [redacted], the Service interviewed a [person] who had engaged in [redacted] chats with him [redacted]. [redacted] [The person] allowed the Service to directly access his [redacted] account, providing the Service written consent and his account credentials. The [redacted] account was accessed and chats between [the person] and [redacted] were reviewed.

[276] Despite [the person] having consented to the Service accessing the [redacted] chats, the question of whether [redacted] retains a reasonable expectation of privacy in that electronic communication arises.

[277] For an action to constitute a search or seizure that engages section 8, the impacted individual must have a reasonable expectation of privacy in the information that the State has accessed (*Hunter* at pgs. 150–160; *Goodwin v British Columbia (Superintendent of Motor Vehicle),* 2015 SCC 46 at para. 55.) A reasonable expectation of privacy is to be determined on the totality of the circumstances (*R v Edwards*, [1996] 1 SCR 128 at para. 45). The analysis is guided by the subject matter in issue, the individual's direct interest and subjective expectation of privacy, and an assessment of the reasonableness of the individual's subjective expectation (*R v Tessling*, 2004 SCC 67 at paras. 31–32; *R v Patrick*, 2009 SCC 17 [*Patrick*] at para. 27; *R v Cole*, 2012 SCC 53 at paras. 40 and 45).

[278] Electronic informational content, including stored electronic communications, may attract a reasonable expectation of privacy (*R v Morelli*, 2010 SCC 8 [*Morelli*]; *R v Telus Communications Co.*, 2013 SCC 16; *R v Marakah*, 2017 SCC 59 [*Marakah*]). In *Marakah* the majority in the Supreme Court found that both parties to an electronic conversation may, depending on the totality of the circumstances, maintain an ongoing reasonable expectation of privacy in that conversation (*Marakah* at para. 5). In determining whether a subjective expectation of privacy is objectively reasonable in the context of an electronic conversation the Supreme Court identified three factors for consideration: (1) the place where the search occurred;

(2) the private nature of the subject matter; and (3) control over the subject matter (*Marakah* at para. 24).

[279] The Supreme Court has also held, in the context of information on a shared computer, that the consent of one party cannot negate the reasonable expectation of privacy the other might have (*R v Reeves*, 2018 SCC 56 [*Reeves*] at para. 41). As noted in *Reeves*, the risk an individual assumes in providing another access to information they would hope to keep private does not negate a reasonable expectation of privacy: "the question is not which risks the claimant has taken, but which risks should be imposed on him in a free and democratic society" (para. 41).

[280] The AGC acknowledges that [redacted] had a subjective expectation of privacy in the [redacted] communication but takes the position that one cannot conclude that there was an objectively reasonable expectation of privacy. The AGC notes that the evidence was obtained [redacted] prior to the Supreme Court of Canada decisions in *Marakah* and *Reeves* and submits that at this point in time the jurisprudence would not have supported a conclusion that [redacted] had a reasonable expectation of privacy in the [redacted] chat. The AGC argues there was sufficient authority for the Service to act as it did [redacted] and further submits the law as it exists today continues to provide sufficient authority for the Service to have accessed the communications without having obtained a warrant.

[281] The *amici* do not take issue with the view that any breach was carried out in good faith. However, they further note that the issue of possible infringement in this instance is complex and

that it is far from clear how the three factor inquiry provided for in *Marakah* would resolve the question of the objective reasonableness of a subjective expectation of privacy on the part of [redacted]. Citing the divergent views expressed by the seven member Court in *Reeves*, the *amici* note the issue is one that is subject to significant jurisprudential refinement in the future.

[282] Whether [redacted] had a reasonable expectation of privacy [redacted] does raise a series of complex questions. I agree with the *amici*: these questions need not be resolved in this case. The contents of the [electronic communication] were excluded from consideration in the granting of the warrants. The circumstances also strongly suggest that the information, even if unlawfully collected, might well be admitted and considered on other grounds. In the circumstances it is neither necessary nor appropriate that I address the issues.

(c) *[Electronic device]*

[283] [In the Service's investigation of one of the targets, a partner provided the Service with an electronic device that had been left behind by the target when the target departed Canada and had subsequently been provided to the partner. The partner advised the Service that it considered the electronic device to have been provided to it on consent and the partner had relied on this consent in accessing the electronic device. The electronic device provided information that the Service used in support of its warrant application.] [redacted]

[284] The AGC concedes that [the person who provided the electronic device to the partner] could not waive [the target's] reasonable privacy expectation but submits that [the target] abandoned his interest in [the electronic device]. The search, it is submitted, did not result in a *Charter* breach.

[285] In *Patrick*, Justice Binnie states at paragraph 25 that abandonment is an issue of fact:

> [25] Abandonment is therefore an issue of fact. The question is whether the claimant to section 8 protection has acted in relation to the subject matter of his privacy claim in such a manner as to lead a reasonable and independent observer to conclude that his continued assertion of a privacy interest is unreasonable in the totality of the circumstances.

[286] I must determine whether the totality of the circumstances lead one to conclude that [the electronic device] was abandoned. In my opinion they do.

[287] Abandonment is a conclusion to be drawn from conduct and the reasonableness of any assertion of an ongoing privacy interest and must be assessed based upon the impacted individual's conduct (*Patrick* at para. 54). [The target] departed Canada [redacted]. He was reported [redacted] as missing. [redacted]. He has told others he has no intention of returning to Canada and there is no contrary indication in the evidence.

[288] Departing the country with the intent to not return is insufficient to conclude that property, particularly [a personal electronic device], had been abandoned. [Personal electronic devices] and their contents engage pronounced privacy interests (*Morelli* at para. 105). However, the evidence of abandonment in this case goes beyond this. The purpose for [the target's] departure, the circumstances surrounding the departure and the circumstance surrounding his ongoing absence from Canada are relevant factors.

[289] The evidence indicates that [the target] was dissatisfied with Canada and no longer wanted to live in Canada. He had adopted a violent interpretation of Islam and wanted to engage in *jihad*. He departed Canada without providing any notice [redacted]. He has claimed he has no intent to return to Canada [redacted]. The totality of these circumstances does allow an independent reasonable observer to conclude that any continued assertion of a privacy interest in the [electronic device] would be unreasonable.

(d) *Disclosure of source identity*

[290] The disclosure of the identity of a human source in a proceeding before a court is prohibited under the *CSIS Act* unless both the human source and the Director consent to the disclosure:

~~**TOP SECRET**~~

***Canadian Security Intelligence Service Act*, RSC, 1985, c. C-23**	***Loi sur le Service canadien du renseignement de sécurité*, LRC (1985), ch. C-23**
Prohibition on disclosure	**Interdiction de communication**
(2) Subject to subsections (3) and (8), no person shall, in a proceeding before a court, person or body with jurisdiction to compel the production of information, disclose the identity of a human source or any information from which the identity of a human source could be inferred.	**(2)** Sous réserve des paragraphes (3) et (8), dans une instance devant un tribunal, un organisme ou une personne qui ont le pouvoir de contraindre à la production d'informations, nul ne peut communiquer l'identité d'une source humaine ou toute information qui permettrait de découvrir cette identité.
Exception — consent	**Exception — consentement**
(3) The identity of a human source or information from which the identity of a human source could be inferred may be disclosed in a proceeding referred to in subsection (2) if the human source and the Director consent to the disclosure of that information.	**(3)** L'identité d'une source humaine ou une information qui permettrait de découvrir cette identité peut être communiquée dans une instance visée au paragraphe (2) si la source humaine et le directeur y consentent.

[291] A human source is defined in the *CSIS Act* as being an individual to whom a promise of confidentiality has been made:

Canadian Security Intelligence Service Act, **RSC, 1985, c. C-23**	*Loi sur le Service canadien du renseignement de sécurité,* **LRC (1985), ch. C-23**
human source means an individual who, after having received a promise of confidentiality, has provided, provides or is likely to provide information to the Service; (source humaine)	**source humaine** Personne physique qui a reçu une promesse d'anonymat et qui, par la suite, a fourni, fournit ou pourrait vraisemblablement fournir des informations au Service. (human source)

[292] [redacted]

[293] The Service complied with this request and in doing so disclosed the identity of a source that was relied upon in [Case A] and [Case B]. The fact that the identity of this source had been disclosed to [a partner] was made known to the Court in the source précis in [Case A]. This raised questions relating to the circumstances and what if any knowledge the source had of the Service's disclosure actions.

[294] That the privilege conferred by section 18.1 does not apply in the circumstances described above was confirmed in the initial hearing. However disclosure of the human source's

identity to [a partner] remained an issue on the basis that it appeared inconsistent with the promise of confidentiality that all human sources must be provided (*CSIS Act*, s. 2).

[295] The AGC submits that identity disclosure in this instance was not material to the decision to issue or refuse the requested warrants as there was no information to suggest the relationship between the source and the Service had any bearing on either credibility or reliability. The AGC further submits that the statutory requirement for a promise of confidentiality is intended to establish the basis upon which a claim of privilege under section 18.1 is to be asserted and assessed in proceedings. The promise does not apply to confidential disclosures undertaken for operational reasons. The AGC argues that the disclosure of the identity of a human source to protect the security of the source in the course of a Service investigation is authorized by subsection 19(2) of the *CSIS Act*. The AGC further argues that where disclosure of identity is made to [a partner, that partner] is brought within the circle of privilege and there is an expectation that [the partner] will protect the identity of the source. Finally the AGC submits that whether a human source is to be advised that his or her identity will be disclosed to [a partner] must be determined after a consideration of what course of action best protects a source's security. The AGC submits that the source's security motivated the disclosure in this instance, that no judicial remedy is warranted and the information provided by the source can be relied upon in support of the application.

[296] Contrary to the AGC's submissions, the circumstances surrounding identity disclosure in this instance were not immaterial to the application. As the AGC has acknowledged, the

circumstances and underlying reasons for disclosure are factors that might well impact upon credibility and reliability. The materiality determination can only be made once the facts and circumstances have been made available to the Court. The improper or unauthorized disclosure of a source's identity might also impact upon the exercise of the warrant granting discretion. Inquiries for the purposes of clarifying the authority to disclose, the purpose of disclosure, and the nature of the security risk in issue are, in my view, relevant and therefore well within the authority of the Court to explore.

[297] I have some reservations with the AGC submissions to the effect that the scope of the promise of confidentiality is limited to the general public and in particular groups and individuals the human source reports upon. I am not convinced that this narrow interpretation of the scope of the promise can be sustained upon a contextual reading of the definition of "human source" at section 2 of the *CSIS Act*, or that it is consistent with the underlying purposes and objectives of assuring sources that their identity will be protected. However I need not determine this issue in this instance.

[298] I am satisfied that a judicial remedy is not required in this instance and the information provided by the source could be relied upon in considering the application.

VI. Waiver of solicitor-client privilege

[299] In addressing the scope of the issues before the Court, the *amici* observed that the witnesses had relied on legal advice to explain their conduct and characterized the waiver as

voluntary. AGC counsel took issue with the waiver being characterized as voluntary, suggesting that the Court influenced the waiver. The AGC sought leave to make further submissions on this point.

[300] Ultimately, AGC counsel did not pursue the request to make further submissions and acknowledged that the Service's waiver of privilege was voluntary. However, in addressing the basis for the initial objection, counsel explained that it arose as the result of judicial interest having been expressed in the legal advice subsequent to the delivery of the Senior General Counsel's letter to the Court in January 2019.

[301] Although the issue has not been pursued, the suggestion that the Court sought to influence the production of privileged legal advice warrants comment.

[302] The Senior General Counsel's letter to the Court in January 2019 enclosed a copy of the "Interim Direction on the Conduct of Operations Likely Involving the Commission of Criminal Offences," as noted above. The Interim Direction states that the issue of illegality has arisen due to "changes in Canada's legal landscape," that the "evolution of the law has resulted in increased legal risk to CSIS employees and human sources," and that the Government has addressed this risk through the creation of a legislative justification regime. During the CMC that followed the January 2019 letter, counsel was asked to identify the changes in Canada's legal landscape referred to in the Interim Direction. Counsel was not requested to disclose legal advice, although

counsel did advise the Court that privilege obligations limited counsel in responding to the Court. The Court respected counsel's comments to this effect.

[303] The Court was advised that the Director of the Service had waived solicitor-client privilege over "relevant legal opinions" with the filing of the January 2019 Affidavit in [Case B]. The potential waiver of solicitor-client privilege had not previously arisen in [Case B].

[304] In the course of the common issues hearings, the *amici* requested additional documents either referenced and relied on in the legal advice over which privilege had been waived or that was relied on by affiants in the course of their evidence. Where this situation arose, counsel for the Service identified any claim of privilege and undertook to obtain instructions. The scope and impact of the Service's initial waiver decision was never placed in issue.

[305] The suggestion that the Court influenced the Service's decision to waive solicitor-client privileged is not tenable. As reflected in the January 2019 Affidavit advising of the waiver, the decision rested with and was made by the Service.

VII. Concluding remarks

[306] In November 2019, the Court was informed of a series of measures the Service had initiated to address access to, and use of, human source information in the warrant preparation and application process. One of the three measures identified was the engagement, in mid-

September 2019, of Mr. Morris Rosenberg, a former senior Deputy Minister. Mr. Rosenberg was engaged to conduct a review of Service practices regarding the disclosure of information about human sources in warrant applications. The review was undertaken in the context of non-disclosure of information relating to a source in [Case D] before Justice Brown.

[307] In March 2020, the Court was advised that Mr. Rosenberg's report had been completed. A copy was subsequently filed by way of Supplemental Affidavit and is titled "Independent Review – Duty of Candour at CSIS." It is limited to a consideration of the circumstances relating to the single source in [Case D] The report is formatted as a presentation, a series of slides with information set out in lists and narrative statements supported by diagrams and charts.

[308] In describing his mandate, Mr. Rosenberg notes that "[p]revious duty of candour reviews conducted by Segal and Sims have focused mainly on DLSU and affiant's dealing with the Federal Court. This review was scoped to focus more specifically on actions that can be taken within the Service to address duty of candour concerns."

[309] The Rosenberg report identifies deficiencies in the areas of internal communications, the relationship between the Department of Justice and the Service and training as contributing to the issues that arose in [Case D] The report notes that a precondition to addressing these deficiencies is "the need to address cultural issues around warrants."

[310] Despite the limited scope of this internally mandated report, institutional culture is identified as undermining both the commitment to and compliance with core values including respect for the rule of law. The report reinforces my view that a comprehensive external review is required. It is another signal that steps must be taken to address these issues. This comprehensive review must encompass Service and Department of Justice processes, governance, culture, and relationships impacting upon compliance with the duty of candour. The review must address more fundamental concerns relating to the prioritization of the rule of law as a foundational principle in all Service decision-making. Mr. Rosenberg's report is another indicator of the need for a comprehensive external review; it should not be seen as a substitute for it.

[311] With respect to the substantive issues that have arisen in this matter I have concluded that:

A. Within the context of an application for warrants pursuant to sections 12 and 21 of the *CSIS Act* the Court may consider information likely collected in contravention of the law. However, such information should only be considered after the Court has considered and weighed all relevant factors. These factors include the seriousness of the likely illegal activity; the circumstances in which likely illegality occurred; the impact of any likely illegality on issues of fairness and individual rights; and broader societal interests that may be engaged. These factors are to be considered and weighed within the broader context of the overall impact a decision to consider or exclude the impugned information would have on the long-term repute of the administration of justice. This analysis should

be considered with a particular focus on the expectation that national security investigations are to be undertaken within the bounds of the law.

B. Where new facts come to light that could have impacted upon the exercise of judicial discretion, the Court has the inherent right to review a previously issued *ex parte* warrant. Where such facts disclose that information likely collected in contravention of the law was placed before the Court, the Court will determine whether any such information should have been considered by engaging in the analysis summarized at paragraph (A). Having reached a conclusion on whether to consider or exclude the impugned information, the Court will then consider whether the Order could have issued based on the information properly before the Court.

C. Should the Court invalidate or otherwise vary a previously issued warrant on the basis that new facts have come to light that could have impacted on the exercise of judicial discretion the Court may also consider remedial measures that would impact on information previously collected pursuant to the invalidated or varied warrant.

D. The discovery or disclosure of significant facts or circumstances in the course of judicial consideration of a warrant application does not vitiate the pre-application consultation and approval process prescribed in the *CSIS Act*. However a designated judge possesses the inherent discretion to decline to issue a warrant pending notification of the subsequently discovered facts or circumstances to appropriate officials or authorities.

~~**TOP SECRET**~~

JUDGMENT

THIS COURT'S JUDGMENT is that:

1. The Canadian Security Intelligence Service breached the duty of candour it owed to the Court in failing to proactively identify and disclose that it had included in support of warrant applications [Case A] and [Case B] information that was likely derived from illegal activities;

2. It is recommended that a comprehensive external review be initiated to fully identify systemic, governance and cultural shortcomings and failures that resulted in the Canadian Security Intelligence Service engaging in operational activity that it has conceded was illegal and the resultant breach of candour. This review should include but not be limited to the following areas of inquiry:

    i. The application of the Department of Justice legal risk assessment framework to Service operations;

    ii. The manner in which legal advice is delivered to the Canadian Security Intelligence Service;

    iii. An assessment of whether legal risk is always an appropriate framework in which to assess and provide advice on the legal consequences of intelligence operations;

iv. The sharing of information within the National Security Litigation and Advisory Group, particularly as between those employees fulfilling an advisory function and those appearing before the Court;

v. The interplay between Service counsel's duty of candour to the Court and their duty of loyalty to the Canadian Security Intelligence Service;

vi. The nature and extent of any duty to act where counsel for the Attorney General is aware that a client is, or probably is, operating contrary to law;

vii. The information security practices followed by the Service to ensure that senior decision-makers and advisors, in reviewing or approving operational activities, can identify relevant linkages between distinct operational initiatives and recognize the potential relevance of other information known to the decision-maker;

viii. Assuring the Court that human source information has been subject to the same rigorous challenge in the warrant preparation process as any other information and that affiants can fully satisfy their duty of candour obligations in respect of human sources of information;

ix. Consideration as to whether individual conduct and decision-making warrants further review or action;

3. Pending consideration of an amendment to the warrant template, the Canadian Security Intelligence Service shall comply with paragraph 241of the enclosed reasons;

4. The Canadian Security Intelligence Service and the Department of Justice shall advise the Court within sixty (60) days as to how it intends to proceed in light of the Court's recommendations;

5. These reasons shall, within twenty (20) days of the date of this judgment and reasons, be reviewed by counsel for the Attorney General and the Canadian Security Intelligence Service for the purposes of identifying what parts of the judgment and reasons can be made public. After those twenty (20) days, and within the following twenty (20) days, the *amici* shall review the suggested redactions. Both are to be guided by the open court principle and shall work cooperatively in conducting this review. Any contentious issues shall be referred to the undersigned within the following five (5) days for determination.

"Patrick Gleeson"

Judge

~~**TOP SECRET**~~

ANNEX A

Appendix 1

OVERVIEW OF EVIDENCE AND PROCEEDINGS

Affiants in [Case B][1]

AFFIANTS			
Affiants Identified by Position	**Affidavit(s) Filed**		**Date(s) Testified**
	Date Sworn or Affirmed	**Date Filed**	
CSIS Intelligence Officer - Deputy Chief Counter Terrorism Division (Applicant in [Case B])	August 23, 2018	September 7, 2018	October 18, 2018
	September 6, 2018	September 7, 2018	February 13, 2019
	November 8, 2018	November 9, 2018	April 3, 2019
	March 8, 2019	March 8, 2019	
	April 1, 2019	April 1, 2019	
	May 28, 2019	May 28, 2019	
CSIS Intelligence Officer – Chief Human Source Management	January 25, 2019	January 25, 2019	February 13, 2019
	January 25, 2019 (Affidavit of Documents in two Volumes)	January 25, 2019	
	February 28, 2019	March 8, 2019	
	November 7, 2019	November 8, 2019	
	March 23, 2020	March 23, 2020	
Legal Assistant	January 25, 2019 (Affidavit of Documents)	January 25, 2019	
NSLAG General Counsel	March 6, 2019	March 15, 2019	April 17, 2019
NSLAG Counsel	March 14, 2019	March 15, 2019	April 29, 2019
	April 23, 2019 (Filed in support of a Motion seeking limited standing)	April 26, 2019	

[1] Additional affidavits were filed and witnesses were heard in [Case D]. Additional affidavits were filed in [Case C]. This evidence is not reflected in this Annex.

~~**TOP SECRET**~~

ANNEX A

Appendix 2

OVERVIEW OF EVIDENCE AND PROCEEDINGS

Hearings and Case Management Conferences [CMCs] in [Case B][2]

HEARINGS AND CASE MANAGEMENT CONFERENCES			
Date	**Hearing or CMC**	**Justices Present**	**Comment**
October 1, 2018	CMC	Justice Gleeson	
October 18, 2018	Hearing	Justice Gleeson	Witness
October 19, 2018	CMC	Justice Gleeson	
November 7, 2018	CMC	Justice Gleeson	
January 14, 2019	CMC	Justice Gleeson	
February 13, 2019	Hearing	Justice Gleeson	Witnesses
March 29, 2019	CMC	Justice Gleeson	
April 3, 2019	Hearing and CMC	Justice Gleeson	Witness
April 17, 2019	Hearing	Justice Gleeson	Witness
April 29, 2019	Hearing	Justice Gleeson	Witness
June 28, 2019	Hearing	Justice Gleeson	Oral Submissions

[2] There were a series of CMCs in [Case A] between April and July 2018 prior to the filing of the fresh application in [Case B] on September 7, 2018.

~~**TOP SECRET**~~

ANNEX A

Appendix 3

OVERVIEW OF EVIDENCE AND PROCEEDINGS

Affiants in the Common Issues Proceedings[3]

AFFIANTS			
Affiants Identified by Position	**Affidavit(s) Filed**		**Date(s) Testified**
	Date Sworn or Affirmed	**Date Filed**	
Director – CSIS (from 2013 to May 2017)	March 14, 2019	March 15, 2019	April 1, 2019 to April 2, 2019
Deputy Director Operations – CSIS (June 2018 to present)	March 17, 2019	March 18, 2019	April 1, 2019 to April 2, 2019
Director – CSIS (June 2017 to present)	March 17, 2019	March 18, 2019	April 1, 2019 to April 2, 2019
Legal Assistant	March 29, 2019	March 29, 2019	
	November 7, 2019	November 8, 2019	
Deputy Director Operations – CSIS (2013 to 2019)	April 24, 2019	April 24, 2019	April 29, 2019
NSLAG General Counsel	April 24, 2019	April 25, 2019	
Executive Director and Senior General Counsel – NSLAG (2009 to 2018)	April 25, 2019 April 29, 2019 (Filed in support of a motion seeking limited standing)	April 25, 2019 April 29, 2019	April 30, 2019 and May 13, 2019
Deputy Minister of Justice and Deputy Attorney General of Canada (June 26, 2017 to present)	June 10, 2019	June 10, 2019	
Deputy Minister of Justice and Deputy Attorney General of Canada	July 5, 2019	July 5, 2019	August 28, 2019

[3] Additional affidavits were filed and witnesses were heard in [Case D]. Additional affidavits were filed in [Case C]. This evidence is not reflected in this Annex.

~~**TOP SECRET**~~

ANNEX A

Appendix 3

AFFIANTS			
Affiants Identified by Position	**Affidavit(s) Filed**		**Date(s) Testified**
	Date Sworn or Affirmed	**Date Filed**	
(November 5, 2012 to June 23, 2017)			
Assistant Deputy Minister of Public Safety, Defence and Immigration (2014 to present)	August 8, 2018	August 9, 2018	August 28, 2019
CSIS Intelligence Officer – Chief Human Source Management	November 7, 2019	November 8, 2019	
	March 23, 2020	March 23, 2020	

~~**TOP SECRET**~~

ANNEX A

Appendix 4

OVERVIEW OF EVIDENCE AND PROCEEDINGS

Hearings and Case Management Conferences [CMCs] in the Common Issues Proceedings

HEARINGS AND CASE MANAGEMENT CONFERENCES			
Date	**Hearing or CMC**	**Justices Present**	**Comment**
January 28, 2019	CMC	Justices Mosley and Kane	
February 21, 2019	Hearing	*En Banc*	
April 1, 2019	Hearing	Justices Brown and Gleeson	Witnesses
April 2, 2019	Hearing	Justices Brown and Gleeson	Witnesses
April 12, 2019	CMC	Justices Kane, Brown and Gleeson	
April 29, 2019	Hearing	Justices Kane, Brown and Gleeson	Witness
April 30, 2019	Hearing	Justices Kane, Brown and Gleeson	Witness
May 13, 2019	Hearing	Justices Kane, Brown and Gleeson	Witness
May 29, 2019	Hearing	Justices Kane, Brown and Gleeson	
June 27, 2019	Hearing	Justices Kane, Brown and Gleeson	Oral Submissions
July 30, 2019	CMC	Justices Kane, Brown and Gleeson	
August 28, 2019	Hearing	Justices Kane, Brown and Gleeson	Witnesses
November 1, 2019	Hearing	Justices Brown and Gleeson	Oral Submissions

~~**TOP SECRET**~~

ANNEX A

Appendix 5

OVERVIEW OF EVIDENCE AND PROCEEDINGS

Legal Opinions

LEGAL OPINIONS			
Date	**Authored by**	**Addressed to**	**Location in Record**
April 5, 2002	Department of Justice Constitutional and Administrative Law Section	Numerous Addressees	NSLAG Legal Assistant Affidavit of Documents filed March 29, 2019
April 28, 2005	NSLAG	Numerous Service Addressees	NSLAG Legal Assistant Affidavit of Documents filed March 29, 2019
April 11, 2013	NSLAG	Senior General Counsel NSLAG	NSLAG Legal Assistant Affidavit of Documents filed March 29, 2019
June 29, 2015	Assistant Deputy Minister of Public Safety, Defence and Immigration	Public Safety and CSIS Officials	Assistant Deputy Minister of Public Safety, Defence and Immigration Affidavit filed August 9, 2019
October 8, 2015	NSLAG	Deputy Director Operations CSIS	Deputy Director Operations – CSIS Affidavit filed March 18, 2019
Various opinions prepared in the context of operational legal risk assessments between March 2017 and late 2018	NSLAG	Service	CSIS Intelligence Officer – Chief Human Source Management Affidavit of

~~**TOP SECRET**~~

ANNEX A

Appendix 5

LEGAL OPINIONS			
Date	**Authored by**	**Addressed to**	**Location in Record**
			Documents filed January 25, 2019 and NSLAG General Counsel Affidavit filed April 25, 2019
January 23, 2017	NSLAG	Director CSIS	NSLAG Legal Assistant Affidavit of Documents filed January 25, 2019
February 3, 2017	Draft Opinion prepared for the consideration of the then DM Justice	Drafted to provide to the Director CSIS	Deputy Minister of Justice and Deputy Attorney General of Canada Affidavit filed July 5, 2019
January 7, 2019	Senior General Counsel NSLAG	Director CSIS	NSLAG Legal Assistant Affidavit of Documents filed January 25, 2019

~~**TOP SECRET**~~

ANNEX A

Appendix 6

OVERVIEW OF EVIDENCE AND PROCEEDINGS
Pertinent Security Intelligence Review Committee [SIRC] Reports

SIRC REPORTS			
Report Title	**Report Number**	**Public References**	**Location in Record**
SIRC Review of a Human Source Operation	SIRC Review 2008-04	SIRC Annual Report (2008-2009) pgs. 15-16	Provided under the cover of a letter from Counsel for the AGC dated May 8, 2019 in response to an undertaking
CSIS's Investigation of Canadian Foreign Fighters	SIRC Review 2014-05	SIRC Annual Report (2014-2015) pgs. 15-17.	Referenced in SIRC Annual Report (2014-2015) marked as Exhibit CC 1 on April 1, 2019
CSIS's Relationship and Exchanges with the Department of Foreign Affairs, Trade and Development	SIRC Review 2014-07	SIRC Annual Report (2014-2015) pgs. 17-20 Updated	Filed on April 9, 2019 in response to undertakings
CSIS's investigation of Canadian Foreign Fighters	SIRC Review 2015-09	SIRC Annual Report (2015-2016) pgs.18-20	Marked as Exhibit APP2 on April 1, 2019

~~**TOP SECRET**~~

ANNEX B

***Criminal Code*, RSC, 1985, c. C-46**	***Code Criminel*, LRC (1985), ch. C-46**
PART II.1	**PARTIE II.1**
Terrorism	**Terrorisme**
Interpretation	Interprétation
Definitions	**Définitions**
83.01 (1) The following definitions apply in this Part.	**83.01 (1)** Les définitions qui suivent s'appliquent à la présente partie.
Canadian means a Canadian citizen, a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act* or a body corporate incorporated and continued under the laws of Canada or a province. (*Canadien*)	
entity means a person, group, trust, partnership or fund or an unincorporated association or organization. (*entité*)	
listed entity means an entity on a list established by the Governor in Council under section 83.05. (*entité inscrite*)	
terrorist activity means	***activité terroriste***
(a) an act or omission that is committed in or outside Canada and that, if committed in Canada, is one of the following offences:	**a)** Soit un acte — action ou omission, commise au Canada ou à l'étranger — qui, au Canada, constitue une des infractions suivantes :
(i) the offences referred to in subsection 7(2) that implement the *Convention for the Suppression of Unlawful Seizure of Aircraft*, signed at The Hague on December 16, 1970,	**(i)** les infractions visées au paragraphe 7(2) et mettant en oeuvre la Convention pour la répression de la capture illicite d'aéronefs, signée à La Haye le 16 décembre 1970,
(ii) the offences referred to in subsection 7(2) that implement the *Convention for the* ***Suppression of Unlawful*** *Acts against the*	**(ii)** les infractions visées au paragraphe 7(2) et mettant en oeuvre la *Convention pour la répression d'actes illicites dirigés contre la*

~~TOP SECRET~~

ANNEX B

Safety of Civil Aviation, signed at Montreal on September 23, 1971,

(iii) the offences referred to in subsection 7(3) that implement the *Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents*, adopted by the General Assembly of the United Nations on December 14, 1973,

(iv) the offences referred to in subsection 7(3.1) that implement the *International Convention against the Taking of Hostages*, adopted by the General Assembly of the United Nations on December 17, 1979,

(v) the offences referred to in subsection 7(2.21) that implement the Convention on the Physical Protection of Nuclear Material, done at Vienna and New York on March 3, 1980, as amended by the Amendment to the Convention on the Physical Protection of Nuclear Material, done at Vienna on July 8, 2005 and the International Convention for the Suppression of Acts of Nuclear Terrorism, done at New York on September 14, 2005,

(vi) the offences referred to in subsection 7(2) that implement the *Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation*, supplementary to the *Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation*, signed at Montreal on February 24, 1988,

(vii) the offences referred to in subsection 7(2.1) that implement the *Convention for the Suppression of Unlawful Acts against the*

sécurité de l'aviation civile, signée à Montréal le 23 septembre 1971,

(iii) les infractions visées au paragraphe 7(3) et mettant en oeuvre la *Convention sur la prévention et la répression des infractions contre les personnes jouissant d'une protection internationale, y compris les agents diplomatiques*, adoptée par l'Assemblée générale des Nations Unies le 14 décembre 1973,

(iv) les infractions visées au paragraphe 7(3.1) et mettant en oeuvre la *Convention internationale contre la prise d'otages*, adoptée par l'Assemblée générale des Nations Unies le 17 décembre 1979,

(v) les infractions visées au paragraphe 7(2.21) et mettant en oeuvre la Convention sur la protection physique des matières nucléaires, faite à Vienne et New York le 3 mars 1980, et modifiée par l'Amendement à la Convention sur la protection physique des matières nucléaires, fait à Vienne le 8 juillet 2005, ainsi que la Convention internationale pour la répression des actes de terrorisme nucléaire, faite à New York le 14 septembre 2005,

(vi) les infractions visées au paragraphe 7(2) et mettant en oeuvre le *Protocole pour la répression des actes illicites de violence dans les aéroports servant à l'aviation civile internationale, complémentaire à la Convention pour la répression d'actes illicites dirigés contre la sécurité de l'aviation civile*, signé à Montréal le 24 février 1988,

(vii) les infractions visées au paragraphe 7(2.1) et mettant en oeuvre la *Convention pour la répression d'actes illicites contre la*

ANNEX B

Safety of Maritime Navigation, done at Rome on March 10, 1988,

(viii) the offences referred to in subsection 7(2.1) or (2.2) that implement the *Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf*, done at Rome on March 10, 1988,

(ix) *the offences referred to in subsection 7(3.72) that implement the International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on December 15, 1997, and*

(x) the offences referred to in subsection 7(3.73) that implement the *International Convention for the Suppression of the Financing of Terrorism*, adopted by the General Assembly of the United Nations on December 9, 1999, or

(b) an act or omission, in or outside Canada,

(i) that is committed

(A) in whole or in part for a political, religious or ideological purpose, objective or cause, and

(B) in whole or in part with the intention of intimidating the public, or a segment of the public, with regard to its security, including its economic security, or compelling a person, a government or a domestic or

sécurité de la navigation maritime, conclue à Rome le 10 mars1988,

(viii) les infractions visées aux paragraphes 7(2.1) ou (2.2) et mettant en oeuvre le *Protocole pour la répression d'actes illicites contre la sécurité des plates-formes fixes situées sur le plateau continental*, conclu à Rome le 10 mars 1988,

(ix) les infractions visées au paragraphe 7(3.72) et mettant en oeuvre la *Convention internationale pour la répression des attentats terroristes à l'explosif*, adoptée par l'Assemblée générale des Nations Unies le 15 décembre 1997,

(x) les infractions visées au paragraphe 7(3.73) et mettant en oeuvre la *Convention internationale pour la répression du financement du terrorisme*, adoptée par l'Assemblée générale des Nations Unies le 9 décembre 1999;

b) soit un acte — action ou omission, commise au Canada ou à l'étranger :

(i) d'une part, commis à la fois :

(A) au nom — exclusivement ou non — d'un but, d'un objectif ou d'une cause de nature politique, religieuse ou idéologique,

(B) en vue — exclusivement ou non — d'intimider tout ou partie de la population quant à sa sécurité, entre autres sur le plan économique, ou de contraindre une personne, un gouvernement ou une organisation nationale ou

ANNEX B

an international organization to do or to refrain from doing any act, whether the public or the person, government or organization is inside or outside Canada, and

internationale à accomplir un acte ou à s'en abstenir, que la personne, la population, le gouvernement ou l'organisation soit ou non au Canada,

(ii) that intentionally

(ii) d'autre part, qui intentionnellement, selon le cas :

(A) causes death or serious bodily harm to a person by the use of violence,

(A) cause des blessures graves à une personne ou la mort de celle-ci, par l'usage de la violence,

(B) endangers a person's life,

(B) met en danger la vie d'une personne,

(C) causes a serious risk to the health or safety of the public or any segment of the public,

(C) compromet gravement la santé ou la sécurité de tout ou partie de la population,

(D) causes substantial property damage, whether to public or private property, if causing such damage is likely to result in the conduct or harm referred to in any of clauses (A) to (C), or

(D) cause des dommages matériels considérables, que les biens visés soient publics ou privés, dans des circonstances telles qu'il est probable que l'une des situations mentionnées aux divisions (A) à (C) en résultera,

(E) causes serious interference with or serious disruption of an essential service, facility or system, whether public or private, other than as a result of advocacy, protest, dissent or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses (A) to (C),

(E) perturbe gravement ou paralyse des services, installations ou systèmes essentiels, publics ou privés, sauf dans le cadre de revendications, de protestations ou de manifestations d'un désaccord ou d'un arrêt de travail qui n'ont pas pour but de provoquer l'une des situations

ANNEX B

mentionnées aux divisions (A) à (C).

and includes a conspiracy, attempt or threat to commit any such act or omission, or being an accessory after the fact or counselling in relation to any such act or omission, but, for greater certainty, does not include an act or omission that is committed during an armed conflict and that, at the time and in the place of its commission, is in accordance with customary international law or conventional international law applicable to the conflict, or the activities undertaken by military forces of a state in the exercise of their official duties, to the extent that those activities are governed by other rules of international law. (*activité terroriste)*

Sont visés par la présente définition, relativement à un tel acte, le complot, la tentative, la menace, la complicité après le fait et l'encouragement à la perpétration; il est entendu que sont exclus de la présente définition l'acte — action ou omission — commis au cours d'un conflit armé et conforme, au moment et au lieu de la perpétration, au droit international coutumier ou au droit international conventionnel applicable au conflit ainsi que les activités menées par les forces armées d'un État dans l'exercise de leurs fonctions officielles, dans la mesure où ces activités sont régies par d'autres règles de droit international. (*terrorist activity*)

Canadien Citoyen canadien, résident permanent au sens du paragraphe 2(1) de la <u>*Loi sur l'immigration et la protection des réfugiés*</u> ou personne morale constituée ou prorogée sous le régime d'une loi fédérale ou provinciale. (*Canadian*)

entité Personne, groupe, fiducie, société de personnes ou fonds, ou organisation ou association non dotée de la personnalité morale. (*entity*)

entité inscrite Entité inscrite sur la liste établie par le gouverneur en conseil en vertu de l'article 83.05. (*listed entity*)

terrorist group means

(a) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or

groupe terroriste

a) Soit une entité dont l'un des objets ou l'une des activités est de se livrer à des activités terroristes ou de les faciliter;

~~**TOP SECRET**~~

ANNEX B

(b) a listed entity,

and includes an association of such entities. (*groupe terroriste*)

b) soit une entité inscrite.

Est assimilé à un groupe terroriste un groupe ou une association formé de groupes terroristes au sens de la présente définition. (*terrorist group*)

For greater certainty

(1.1) For greater certainty, the expression of a political, religious or ideological thought, belief or opinion does not come within paragraph (b) of the definition *terrorist activity* in subsection (1) unless it constitutes an act or omission that satisfies the criteria of that paragraph.

Interprétation

(1.1) Il est entendu que l'expression d'une pensée, d'une croyance ou d'une opinion de nature politique, religieuse ou idéologique n'est visée à l'alinéa b) de la définition de *activité terroriste* au paragraphe (1) que si elle constitue un acte — action ou omission — répondant aux critères de cet alinéa.

For greater certainty

(1.2) For greater certainty, a suicide bombing is an act that comes within paragraph (a) or (b) of the definition terrorist activity in subsection (1) if it satisfies the criteria of that paragraph.

Interprétation

(1.2) Il est entendu que l'attentat suicide à la bombe est un acte visé aux alinéas a) ou b) de la définition de *activité terroriste* au paragraphe (1) s'il répond aux critères prévus à l'alinéa en cause.

Facilitation

(2) For the purposes of this Part, facilitation shall be construed in accordance with subsection 83.19(2).

2001, c. 41, ss. 4, 126; 2010, c. 19, s. 1; 2013, c. 13, s. 6.

Facilitation

(2) Pour l'application de la présente partie, faciliter s'interprète en conformité avec le paragraphe 83.19(2).

2001, ch. 41, art. 4 et 126; 2010, ch. 19, art. 1; 2013, ch. 13, art. 6

Financing of Terrorism

Providing or collecting property for certain activities

83.02 Every person is guilty of an indictable offence and liable to imprisonment for a term

Financement du terrorisme

Fournir ou réunir des biens en vue de certains actes

83.02 Est coupable d'un acte criminel passible d'un emprisonnement maximal de

of not more than 10 years who, directly or indirectly, wilfully and without lawful justification or excuse, provides or collects property intending that it be used or knowing that it will be used, in whole or in part, in order to carry out

(a) an act or omission that constitutes an offence referred to in subparagraphs (a)(i) to (ix) of the definition of *terrorist activity* in subsection 83.01(1), or

(b) any other act or omission intended to cause death or serious bodily harm to a civilian or to any other person not taking an active part in the hostilities in a situation of armed conflict, if the purpose of that act or omission, by its nature or context, is to intimidate the public, or to compel a government or an international organization to do or refrain from doing any act.

2001, c. 41, s. 4; 2019, c. 25, s. 15(E).

Providing, making available, etc., property or services for terrorist purposes

83.03 Every person is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years who, directly or indirectly, collects property, provides or invites a person to provide, or makes available property or financial or other related services

(a) intending that they be used, or knowing that they will be used, in whole or in part, for the purpose of

dix ans quiconque, directement ou non, fournit ou réunit, délibérément et sans justification ou excuse légitime, des biens dans l'intention de les voir utiliser — ou en sachant qu'ils seront utilisés — en tout ou en partie, en vue :

a) d'un acte — action ou omission — qui constitue l'une des infractions prévues aux sous-alinéas a)(i) à (ix) de la définition de *activité terroriste* au paragraphe 83.01(1);

b) de tout autre acte — action ou omission — destiné à causer la mort ou des dommages corporels graves à une personne qui ne participe pas directement aux hostilités dans une situation de conflit armé, notamment un civil, si, par sa nature ou son contexte, cet acte est destiné à intimider la population ou à contraindre un gouvernement ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque.

2001, ch. 41, art. 4; 2019, ch. 25, art. 15(A).

Fournir, rendre disponibles, etc. des biens ou services à des fins terroristes

83.03 Est coupable d'un acte criminel passible d'un emprisonnement maximal de dix ans quiconque, directement ou non, réunit des biens ou fournit — ou invite une autre personne à le faire — ou rend disponibles des biens ou des services financiers ou connexes :

a) soit dans l'intention de les voir utiliser — ou en sachant qu'ils seront utilisés — , en tout ou en partie, pour

ANNEX B

facilitating or carrying out any terrorist activity, or for the purpose of benefiting any person who is facilitating or carrying out such an activity, or

(b) knowing that, in whole or part, they will be used by or will benefit a terrorist group.

2001, c. 41, s. 4; 2019, c. 25, s. 16(E).

[…]

Participating, Facilitating, Instructing and Harbouring

Participation in activity of terrorist group

83.18 (1) Every person who knowingly participates in or contributes to, directly or indirectly, any activity of a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years.

Prosecution

(2) An offence may be committed under subsection (1) whether or not

(a) a terrorist group actually facilitates or carries out a terrorist activity;

(b) the participation or contribution of the accused actually enhances the

une activité terroriste, pour faciliter une telle activité ou pour en faire bénéficier une personne qui se livre à une telle activité ou la facilite;

b) soit en sachant qu'ils seront utilisés, en tout ou en partie, par un groupe terroriste ou qu'ils bénéficieront, en tout ou en partie, à celui-ci.

2001, ch. 41, art. 4; 2019, ch. 25, art. 16(A).

[…]

Participer, faciliter, donner des instructions et héberger

Participation à une activité d'un groupe terroriste

83.18 (1) Quiconque, sciemment, participe à une activité d'un groupe terroriste, ou y contribue, directement ou non, dans le but d'accroître la capacité de tout groupe terroriste de se livrer à une activité terroriste ou de la faciliter est coupable d'un acte criminel passible d'un emprisonnement maximal de dix ans.

Poursuite

(2) Pour que l'infraction visée au paragraphe (1) soit commise, il n'est pas nécessaire :

a) qu'une activité terroriste soit effectivement menée ou facilitée par un groupe terroriste;

b) que la participation ou la contribution de l'accusé accroisse effectivement la capacité d'un groupe

ANNEX B

ability of a terrorist group to facilitate or carry out a terrorist activity; or

(c) the accused knows the specific nature of any terrorist activity that may be facilitated or carried out by a terrorist group.

Meaning of participating or contributing

(3) Participating in or contributing to an activity of a terrorist group includes

(a) providing, receiving or recruiting a person to receive training;

(b) providing or offering to provide a skill or an expertise for the benefit of, at the direction of or in association with a terrorist group;

(c) recruiting a person in order to facilitate or commit

(i) a terrorism offence, or

(ii) an act or omission outside Canada that, if committed in Canada, would be a terrorism offence;

(d) entering or remaining in any country for the benefit of, at the direction of or in association with a terrorist group; and

terroriste de se livrer à une activité terroriste ou de la faciliter;

c) que l'accusé connaisse la nature exacte de toute activité terroriste susceptible d'être menée ou facilitée par un groupe terroriste.

Participation ou contribution

(3) La participation ou la contribution à une activité d'un groupe terroriste s'entend notamment :

a) du fait de donner ou d'acquérir de la formation ou de recruter une personne à une telle fin;

b) du fait de mettre des compétences ou une expertise à la disposition d'un groupe terroriste, à son profit ou sous sa direction, ou en association avec lui, ou d'offrir de le faire;

c) du fait de recruter une personne en vue de faciliter ou de commettre une infraction de terrorisme ou un acte à l'étranger qui, s'il était commis au Canada, constituerait une telle infraction;

d) du fait d'entrer ou de demeurer dans un pays au profit ou sous la direction d'un groupe terroriste, ou en association avec lui;

ANNEX B

(e) making oneself, in response to instructions from any of the persons who constitute a terrorist group, available to facilitate or commit

(i) a terrorism offence, or

(ii) an act or omission outside Canada that, if committed in Canada, would be a terrorism offence.

Factors

(4) In determining whether an accused participates in or contributes to any activity of a terrorist group, the court may consider, among other factors, whether the accused

(a) uses a name, word, symbol or other representation that identifies, or is associated with, the terrorist group;

(b) frequently associates with any of the persons who constitute the terrorist group;

(c) receives any benefit from the terrorist group; or

(d) repeatedly engages in activities at the instruction of any of the persons who constitute the terrorist group.

2001, c. 41, s. 4; 2019, c. 25, s. 20

[…]

e) du fait d'être disponible, sous les instructions de quiconque fait partie d'un groupe terroriste, pour faciliter ou commettre une infraction de terrorisme ou un acte à l'étranger qui, s'il était commis au Canada, constituerait une telle infraction.

Facteurs

(4) Pour déterminer si l'accusé participe ou contribue à une activité d'un groupe terroriste, le tribunal peut notamment prendre en compte les faits suivants :

a) l'accusé utilise un nom, un mot, un symbole ou un autre signe qui identifie le groupe ou y est associé;

b) il fréquente quiconque fait partie du groupe terroriste;

c) il reçoit un avantage du groupe terroriste;

d) il se livre régulièrement à des activités selon les instructions d'une personne faisant partie du groupe terroriste.

2001, ch. 41, art. 4; 2019, ch. 25, art. 20

[…]

~~**TOP SECRET**~~

ANNEX B

Leaving Canada to participate in activity of terrorist group

83.181 Every person who leaves or attempts to leave Canada, or goes or attempts to go on board a conveyance with the intent to leave Canada, for the purpose of committing an act or omission outside Canada that, if committed in Canada, would be an offence under subsection 83.18(1) is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years.

2013, c. 9, s. 6; 2019, c. 25, s. 21

Quitter le Canada : participation à une activité d'un groupe terroriste

83.181 Quiconque quitte ou tente de quitter le Canada — ou monte ou tente de monter dans un moyen de transport dans l'intention de quitter le Canada — dans le but de commettre un acte à l'étranger qui, s'il était commis au Canada, constituerait l'infraction visée au paragraphe 83.18(1) est coupable d'un acte criminel passible d'un emprisonnement maximal de dix ans.

2001, ch. 41, art. 4; 2019, ch. 25, art. 20

Facilitating terrorist activity

83.19 (1) Every one who knowingly facilitates a terrorist activity is guilty of an indictable offence and liable to imprisonment for a term not exceeding fourteen years.

Facilitation

(2) For the purposes of this Part, a terrorist activity is facilitated whether or not

(a) the facilitator knows that a particular terrorist activity is facilitated;

(b) any particular terrorist activity was foreseen or planned at the time it was facilitated; or

(c) any terrorist activity was actually carried out.

2001, c. 41, s. 4

Facilitation d'une activité terroriste

83.19 (1) Est coupable d'un acte criminel passible d'un emprisonnement maximal de quatorze ans quiconque sciemment facilite une activité terroriste

Facilitation

(2) Pour l'application de la présente partie, il n'est pas nécessaire pour faciliter une activité terroriste :

a) que l'intéressé sache qu'il se trouve à faciliter une activité terroriste en particulier;

b) qu'une activité terroriste en particulier ait été envisagée au moment où elle est facilitée;

c) qu'une activité terroriste soit effectivement mise à exécution.

2001, ch. 41, art. 4

ANNEX B

Leaving Canada to facilitate terrorist activity

83.191 Everyone who leaves or attempts to leave Canada, or goes or attempts to go on board a conveyance with the intent to leave Canada, for the purpose of committing an act or omission outside Canada that, if committed in Canada, would be an offence under subsection 83.19(1) is guilty of an indictable offence and liable to imprisonment for a term of not more than 14 years.

2013, c. 9, s. 7

Quitter le Canada : facilitation d'une activité terroriste

83.191 Est coupable d'un acte criminel passible d'un emprisonnement maximal de quatorze ans quiconque quitte ou tente de quitter le Canada — ou monte ou tente de monter dans un moyen de transport dans l'intention de quitter le Canada — dans le but de commettre un acte à l'étranger qui, s'il était commis au Canada, constituerait l'infraction visée au paragraphe 83.19(1).

2013, ch. 9, art. 7

~~**TOP SECRET**~~

ANNEX C

ACTIVITIES AT ISSUE IN THE UNDERLYING MATTERS

[Case B] IN THE MATTER OF ISLAMIST TERRORISM, [redacted]				
Type of assistance	**Specific activity**	**Contravention of Criminal Code (y/n)**	**References**	**Occurred before /after issuance of warrants**
[Provision of funds]	CSIS provided [payments over a few years, totalling less than $25,000, to an individual known to be facilitating or carrying out terrorism]	**Yes – s. 83.03** Provision of money to a person known to be facilitating or carrying out terrorist activity	[redacted]	[redacted]
[Provision of funds]	[redacted] provided [a target with less than $5,000 payment for services]	**Depends – s. 83.03** Depending on the application of *Hinchey* to s. 83.03. The [redacted] may not have conferred a benefit on the recipient.	[redacted]	[redacted]
[Provision of funds]	[redacted] at the direction of the	**Yes – s. 83.03** Provision of money to a	[redacted]	[redacted].

~~**TOP SECRET**~~

ANNEX C

[Case B] **IN THE MATTER OF ISLAMIST TERRORISM,** [redacted]				
Type of assistance	**Specific activity**	**Contravention of Criminal Code (y/n)**	**References**	**Occurred before /after issuance of warrants**
	Service, provided a payment of [less than $1000 to a target]	person known to be facilitating or carrying out terrorist activity.	[redacted]	[redacted]
[Provision of funds]	CSIS' direction to [redacted] to provide [a target with payment for services] [redacted]	**Yes – s. 83.03** Provision of money to a person known to be facilitating or carrying out terrorist activity.	[redacted]	[redacted]
[Provision of funds]	Interrupted transfer of funds [redacted] to [a target]	**No –** No property is provided to the subject of investigation's benefit where a transfer of funds is deliberately interrupted prior to its receipt by the person involved in terrorist activity	[redacted]	[redacted]
[Provision of funds]	[A financial benefit valued at less than $20] was	**Yes – s. 83.03** Provision of	[redacted]	[redacted]

~~**TOP SECRET**~~

ANNEX C

[Case B] **IN THE MATTER OF ISLAMIST TERRORISM,** [redacted]				
Type of assistance	**Specific activity**	**Contravention of Criminal Code (y/n)**	**References**	**Occurred before /after issuance of warrants**
	provided to [a target] by [redacted]	money to a person known to be facilitating or carrying out terrorist activity.		
Provision of goods	CSIS directed [redacted] to provide [a target with goods valued at less than $2,000]. [redacted]	**Yes – s. 83.03** Provision of personal property to a person known to be facilitating or carrying out terrorist activity.	[redacted]	[redacted]

~~**TOP SECRET**~~

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CONF-1-20
STYLE OF CAUSE:	**IN THE MATTER** of an application by [redacted] for warrants pursuant to sections 12 and 21 of the *Canadian Security Intelligence Service Ac*t, RSC 1985, c. C-23 **AND IN THE MATTER** OF Islamist Terrorism, [redacted]
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING (IN CAMERA, EX PARTE):	October 1, 18-19, 2018; November 7, 2018; January 14 and 28, 2019; February 13 and 21, 2019; March 29, 2019 April 1-3, 12, 17, 29 and 30, 2019; May 13 and 29, 2019; June 27-28, 2019; July 30, 2019; August 28, 2019 November 1, 2019.
JUDGMENT AND REASONS:	GLEESON J.
DATED:	MAY 15, 2020

APPEARANCES:

Mr. Robert Frater, Q.C. Mr. Owen Rees Ms. Gabrielle White Ms. Helene Robertson Ms. Nathalie Benoit Ms. Jennifer Poirier Ms. Stéphanie Dion	FOR THE ATTORNEY GENERAL OF CANADA
Mr. Gordon Cameron	*AMICUS CURIAE*
Mr. Matthew Gourlay	*AMICUS CURIAE*

Mr. Anil Kapoor	REPRESENTING AFFIANT
Mr. Dana Achtemichuk	GRANTED LIMITED
Mr. Brian Gover	STANDING IN THE HEARINGS
Mr. Stephen Aylward	
Mr. Donald Bayne	

SOLICITORS OF RECORD:

Attorney General of Canada	FOR THE APPLICANT
Mr. Gordon Camerson	*AMICI CURIAE*
Mr. Matthew Gourlay	