Federal Court Cour fédérale

~~**TOP SECRET**~~

Date: 20260220

Docket: CSIS 24-22

Citation: 2026 FC 242

Ottawa, Ontario, February 20, 2026

PRESENT: The Honourable Mr. Justice Gleeson

BETWEEN:

IN THE MATTER OF AN APPLICATION BY [...] 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 AND [...]

ORDER AND REASONS

I. Introduction

[1] In furthering its investigation into Islamist Terrorism and [...] threat-related activities, the Canadian Security Intelligence Service [CSIS or Service] brought an application seeking:

a. Warrants to investigate the threat-related activities of [...];

b. An Identifying Information warrant [II Warrant] in relation to Canadian selectors [...]; and

c. A provisional post-acquisition device examination warrant [Provisional Device Examination Warrant] to allow the Service to examine forensic copies of four devices in Service holdings that were obtained in the course of coalition military operations [...] and subsequently provided to the Service by the [...].

[2] In seeking the warrants against [...] the Service relied in part on reporting provided by [...] that had been derived from information and material collected by coalition military forces in the conduct of operations targeting violent extremist organizations in countries [...]. This material is referred to as Collected Exploitable Material [CEM], which can include any tangible object of potential intelligence value. In the context of this Application, the meaning of CEM is much narrower – it refers only to digital devices such as cell phones, SIM cards, hard drives, and tablets [Bulk CEM]. Reporting derived from Bulk CEM which has been processed to identify information of intelligence value is referred to as Processed CEM, which is described below at paragraphs 21 to 25.

[3] In this Application, the Service relied in part upon [...] reporting derived from Processed CEM to support the application for warrants against [...]. Processed CEM was also the source of certain of the Canadian selectors for which the II Warrant was sought. The Provisional Device Examination Warrant was sought to allow the Service to exploit four forensic copies of devices in the Service's possession. These four devices, shared with the Service [...], form part of the Service's Bulk CEM holdings.

[4] The Service's reliance on Processed CEM [...] in seeking warrants is not novel. In Court Docket CSIS 19-19, an Identifying Information warrant was issued based, at least in part, on Processed CEM [...]. However, the Service's receipt and exploitation of Bulk CEM – in this instance, four forensic copies of cell phones and their associated SIM cards and SD cards [Devices] – in furthering its section 12 investigation is novel.

[5] The Application raises the issues of whether the *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*] applies to the collection of shared CEM, its receipt by the Service or the Service's use or exploitation of that CEM, and, if the *Charter* does apply, whether section 8 is engaged.

[6] To allow the Court to consider the legal issues raised in the Application with the benefit of any additional evidence, full legal argument, and the assistance of an *amicus curiae* but not unnecessarily compromise the Service's interest in advancing its national security investigation, counsel for the Attorney General of Canada [AGC] proposed, and the Court agreed, that a bifurcated approach be adopted.

[7] In Phase 1, the Court considered the application for warrants including the Provisional Device Examination Warrant which the Service sought out of caution. Following an *ex parte* hearing on December 8, 2022, the warrants were issued with some modification.

[8] Mr. Matthew Gourlay was subsequently appointed as *amicus curiae* to assist the Court in the second phase of the bifurcated process. The Service filed additional evidence, and both the Service and *amicus* filed written submissions. An oral hearing was conducted in June 2023. Following the issuance of the Supreme Court of Canada's decision in *R v Bykovets*, 2024 SCC 6 [*Bykovets*], in which the Court addressed whether an IP address attracts a reasonable expectation of privacy, a further "common issues hearing" was conducted on October 15, 2024, with Justice Catherine Kane who is seized with Court Docket C-1-24.

[9] The issues arising from *Bykovets*, which are of collateral relevance to the issues raised in this matter, were canvassed and addressed by Justice Kane in C-1-24 (2025 FC 1978). Having reviewed Justice Kane's reasons, I am satisfied I need not further address those issues here.

[10] In light of the evidence and for the reasons that follow, I have concluded that:

A. The *Charter* does not apply to the collection of CEM by foreign coalition partners operating in a foreign state, to the Service's receipt of either Processed or Bulk CEM from a foreign agency partner, [...], nor to the Service's use of Processed CEM.

B. Where the Service, in furtherance of an investigation pursuant to section 12 of the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*], seeks to exploit Bulk CEM by accessing or inspecting the contents of the forensic copy of a digital device in furtherance of a domestic investigation involving a person who has a nexus to Canada, the *Charter* applies and section 8 is engaged.

C. The exploitation of the Devices in this case is a search within the meaning of section 8 of the *Charter* that is more than minimally intrusive, requiring prior judicial authorization.

D. The Service's Bulk CEM holdings, assessed as being threat-related information, are not subject to the "dataset" regime provided for in sections 11.01-11.25 of the *CSIS Act*.

II. Background

[11] Before addressing the issues that arise, an overview of the evidence describing the circumstances in which CEM is collected, processed, and shared will be helpful. The summary that follows is based on the evidence of [...]

A. [...]

[12] Further to Canada's international obligation to strengthen international cooperation to address the threat posed by foreign terrorist fighters, [...]

[13] [Describes the framework governing the collection, processing, and sharing of CEM]

[14] [Describes the framework governing the collection, processing, and sharing of CEM]

[15] [Describes the framework governing the collection, processing, and sharing of CEM]

[16] [Describes the framework governing the collection, processing, and sharing of CEM]

B. *CEM Collection and Service Access to CEM*

[17] CEM is collected in the course of what [...] has described as targeted military operations [...]. In response to Service queries, senior [...] representatives [...] have advised the Service that the targeted operations in which the CEM in issue was collected were undertaken in accordance with [...] domestic law and applicable international law including international humanitarian law.

[18] [Describes CEM processing]

[19] [...] capable of accessing the data on collected devices and generating unaltered forensic copies of the device that are reported to be of a quality and produced in a manner that renders the forensic copies admissible in judicial proceedings, [...]. These forensic copies are referred to as a "gold copy" of the original device.

[20] [Describes processed CEM and the means by which it is shared]

(1) [...]

[21] [Describes processed CEM and the means by which it is shared]

[22] [Describes processed CEM and the means by which it is shared]

[23] Where the Service, [...] identifies Canadian nexus information, the Service's operational holdings will be queried. Where the Canadian nexus information has some link to previously reported information or does not appear in Service holdings, a report will be generated by the Service representative [...], [...] and uploaded to Service holdings. In the course of generating this report, further information may be sought [...] about the device or the circumstances in which the device was obtained or captured [...].

(2) [...]

[24] [Describes processed CEM and the means by which it is shared]

[25] [Describes processed CEM and the means by which it is shared]

(3) [...]

[26] [Describes processed CEM and the means by which it is shared]

[27] [Describes processed CEM and the means by which it is shared]

(4) [...]

[28] [Describes processed CEM and the means by which it is shared]

(5) The Service's Collection of Gold Copies

[29] In addition to the Service's access to Processed CEM as set out above, [...] has provided the Service with [...] gold copies of Bulk CEM. [...] the Service possesses [...] gold copies [Bulk CEM Holdings].

[30] The Bulk CEM Holdings are controlled and managed by the Service's [...] Branch. [...]

[31] In addition to the receipt of gold copies, when conducting a particular Service investigation, the Service may request a specific device gold copy [...]. In this matter, the Service did just this; it requested and received three gold copies that were in the possession of [...]. The Provisional Device Examination Warrant sought and issued authorizes the Service to exploit these three Devices. The fourth Device the Service sought to exploit formed part of the Service's Bulk CEM Holdings. Authorization to exploit this Device was denied pending consideration of the application of the "dataset" regime to the Service's Bulk CEM Holdings.

C. *The Source of CEM-Derived Information Relied on in the Application for Warrants*

[32] The CEM-derived information relied on in this Application was obtained in the course of [...] operations [...]. [...].

III. Issues

[33] The legal issues that arise have been broadly framed as follows:

A. Whether the Service's receipt of CEM collected by foreign agencies outside Canada as part of interagency information sharing and in furtherance of its mandate pursuant to section 12 of the *CSIS Act* engages section 8 privacy interests under the *Charter*.

B. If so, whether this non-warranted collection activity is authorized as a minimally intrusive form of search by section 12 of the *CSIS Act*.

C. Whether information collected by the Service as part of its Bulk CEM Holdings is subject to the "dataset" regime provided for in sections 11.01-11.25 of the *CSIS Act*.

[34] To facilitate my analysis, I have reframed the issues:

1. Where the Service receives either Processed or Bulk CEM collected by foreign agencies outside Canada as part of interagency information sharing arrangements in furtherance of its mandate pursuant to section 12 of the *CSIS Act*, does the *Charter* apply to:

    i. the foreign agency collection of CEM?

    ii. the Service's receipt and use of Processed CEM?

    iii. the Service's receipt and use or exploitation of Bulk CEM?

2. If the *Charter* applies at any of the above stages, are section 8 privacy rights engaged?

3. If section 8 privacy rights are engaged, is the non-warranted activity authorized as a minimally intrusive form of search by section 12 of the *CSIS Act*?

4. Is the information collected by the Service as part of its Bulk CEM Holdings subject to the "dataset" regime provided for in sections 11.01-11.25 of the *CSIS Act*?

IV. Analysis

A. *The* Charter *in the National Security Context*

(1) The Extraterritorial Application of the *Charter*

[35] In *R v Hape*, 2007 SCC 26 [*Hape*], the Supreme Court of Canada considered whether the *Charter* applies to extraterritorial searches and seizures by Canadian police officers involved in the conduct of an investigation abroad. The starting point when considering the application of the *Charter* is subsection 32(1), which states:

32 (1) This Charter applies	**32. (1)** La présente charte s'applique :
(a) to the Parliament and government of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon Territory and Northwest Territories; and	**a)** au Parlement et au gouvernement du Canada, pour tous les domaines relevant du Parlement, y compris ceux qui concernent le territoire du Yukon et les territoires du Nord-Ouest;
(b) to the legislature and government of each	**b)** à la législature et au gouvernement de chaque

province in respect of all matters within the authority of the legislature of each province.	province, pour tous les domaines relevant de cette législature.

[36] Subsection 32(1) serves to limit the legislative and executive powers of Canada and each of the provinces – it is Parliament, the federal government, and the provinces that are required to comply with the *Charter* "in respect of all matters within [their] authority." Justice LeBel, speaking on behalf of the majority in *Hape*, found the *Charter* cannot, for practical reasons, apply to searches and/or seizures in foreign jurisdictions, noting:

a. in *Schreiber v Canada (Attorney General)*, [1998] 1 SCR 841 [*Schreiber*], it was held sufficient for *Charter* purposes that Canadian officials conducting a search and seizure in a foreign jurisdiction comply with the domestic law of that jurisdiction (*Hape* at para 88).

b. the view in *Schreiber* was followed, at least in part, because, in the context of a search and seizure, an individual's reasonable expectation of privacy would be commensurate with the degree of protection provided by the law in the jurisdiction the individual was located (*Hape* at para 88).

c. this being so, applying the *Charter* in these circumstances affords no additional protection but would create practical obstacles to the conduct of a cooperative investigation where foreign authorities cannot be required to comply with Canadian law (*Hape* at paras 88–89).

d. that Canadian officials may be involved in a cooperative investigation in a foreign jurisdiction is insufficient to render the *Charter* of application because the activity in question – an investigation being undertaken within the foreign territory and pursuant to that state's jurisdiction – is not a matter within the authority of Parliament or the provinces (*Hape* at para 94; also see *Schreiber* at paras 29–30 where Justice L'Heureux-Dubé reinforces that it is the search and seizure which triggers section 8 rights, not any preliminary or preparatory actions by Canadian

> officials that fall short of invading the right to be secure against unreasonable search or seizure).

[37] Justice LeBel concludes at paragraph 90:

> […] The only reasonable approach is to apply the law of the state in which the activities occur, subject to the *Charter*'s fair trial safeguards and to the limits on comity that may prevent Canadian officers from participating in activities that, though authorized by the laws of another state, would cause Canada to be in violation of its international obligations in respect of human rights.

[38] Justice LeBel then summarizes the methodology for determining whether the *Charter* is to be applied to a foreign investigation, stating:

> [113] The methodology for determining whether the *Charter* applies to a foreign investigation can be summarized as follows. The first stage is to determine whether the activity in question falls under s. 32(1) such that the *Charter* applies to it. At this stage, two questions reflecting the two components of s. 32(1) must be asked. First, is the conduct at issue that of a Canadian state actor? Second, if the answer is yes, it may be necessary, depending on the facts of the case, to determine whether there is an exception to the principle of sovereignty that would justify the application of the *Charter* to the extraterritorial activities of the state actor. In most cases, there will be no such exception and the *Charter* will not apply. The inquiry would then move to the second stage, at which the court must determine whether evidence obtained through the foreign investigation ought to be excluded at trial because its admission would render the trial unfair.

[39] This methodology is set out in the context of a criminal investigation. However, there is no reason to limit the *Hape* methodology to criminal investigations or indeed not apply it in the national security context where the Service relies on information or material received from

foreign partners, as contemplated by section 17 of the *CSIS Act*, to assist it in fulfilling its section 12 mandate.

[40] The Supreme Court's interpretation of section 32 of the *Charter* and its application of interpretative and jurisdictional principles of international law in *Hape* were challenged in *R v McGregor*, 2023 SCC 4 [*McGregor*]. In concurring reasons, Justices Karakatsanis and Martin found – within the specific context of the facts before the Court in that case – that section 32 of the *Charter* draws no distinction between domestic and extraterritorial application of the *Charter* and imposes no impediment to the extraterritorial application of the *Charter* as a constraint on Canadian officials inside or outside Canada (*McGregor* at para 55). However, the majority in *McGregor* found *Hape* was not properly before the Court, and reaffirmed *Hape*.

[41] *Hape* remains authoritative on the issue of the extraterritorial application of the *Charter* to investigative activities undertaken by foreign authorities outside of Canada.

(2) Section 8 Engagement

[42] Section 8 of the *Charter* provides:

8 Everyone has the right to be secure against unreasonable search and seizure.	**8** Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

[43] As held by former Chief Justice Paul Crampton in *Canadian Security Intelligence Service Act (Re)*, 2022 FC 1444 [*Outside Canada*], the term "everyone" does not extend to persons who

have no nexus to Canada (at para 153). Only persons with a recognized nexus to Canada can assert section 8 protections. A recognized nexus arises in three instances – where (1) persons are physically within Canada, (2) persons are Canadian citizens, and (3) persons are subject to Canadian criminal proceedings (*Outside Canada* at para 171).

[44] In this instance, the evidence demonstrates that [...] has been present in Canada since [...] and therefore satisfied the nexus to Canada requirement at the time this Application was brought by the Service.

[45] I pause to note that this Court (*X (Re)*, 2017 FC 1047 at para 171) and the Supreme Court (*Hunter et al v Southam Inc*, [1984] 2 SCR 145 at 168 [*Hunter*]) have signalled that section 8 privacy interests might be lessened in the national security context. That being so, there is no basis upon which one might conclude that a different, and in particular a heightened, standard for *Charter* application or section 8 engagement is to be applied in the national security context.

[46] This is particularly so where Canada's national security interests are served and advanced by a robust framework that allows for meaningful international cooperation, including effective interagency sharing of threat-related information. Effective international sharing must recognize the principle of comity and avoid imposing Canadian constitutional requirements on international partners as a condition of effecting international cooperation and information sharing (*Kindler v Canada (Minister of Justice)*, [1991] 2 SCR 779 at 846). In this regard, judicial acknowledgment of the public interest in robust interagency sharing, particularly among

Five Eyes partners, was recently restated by Chief Justice Crampton in *Outside Canada*, where he wrote:

> [103] The public interest in CSIS being able to share information with foreign partners has been repeatedly recognized by this Court and by the Federal Court of Appeal (F.C.A.): see for example, *Mahjoub (Re)*, 2013 FC 1096, 457 F.T.R. 1, at paragraphs 57-58 and 63; *Canada (Attorney General) v. Almalki*, 2010 FC 1106, [2012] 2 F.C.R. 508, at paragraph 131; and *Canada (Attorney General) v. Charkaoui*, 2018 FC 849, at paragraphs 151 and 155. The F.C.A. has also noted the importance of the "give to get" principle: *Mahjoub v. Canada (Citizenship and Immigration)*, 2017 FCA 157, [2018] 2 F.C.R. 344 (*Mahjoub FCA*), at paragraph 287. This principle was also implicitly recognized by the S.C.C. in the context of Canada being a "net importer" of national security information, where the Court noted the state's interest in preserving Canada's present supply of intelligence received from foreign sources: *Ruby v. Canada (Solicitor General)*, 2002 SCC 75, [2002] 4 S.C.R. 3, at paragraphs 43-44.

B. *Does the* Charter *apply to the foreign collection of CEM, to the Service's receipt or exploitation of either Processed or Bulk CEM and, if so, is section 8 engaged?*

[47] The Service and *amicus* rely on *Hape* in adopting the shared position that the *Charter*, and in turn section 8, does not apply to the collection of CEM by military forces operating in foreign jurisdictions where that CEM is ultimately shared with the Service in either a Processed or Bulk form. This is so whether the CEM is passively shared with the Service or is provided from existing [...] holdings in response to a specific Service query, and even if the CEM is believed to contain personal or private information relating to persons who might otherwise benefit from protection under section 8 of the *Charter*.

[48] However, unlike the Service, the *amicus* submits that despite the non-application of the *Charter* to the collection or Service receipt of Processed or Bulk CEM, the *Charter* does apply where the Service may subsequently seek to exploit Bulk CEM in furthering a domestic intelligence investigation. This on the basis that where the reasonable expectation of privacy of a potential section 8 rights-holder may be impacted by the Service's exploitation of Bulk CEM, that rights-holder has a residual privacy interest in the Bulk CEM and that interest engages section 8 of the *Charter*.

[49] I address these arguments by considering the issues of *Charter* application and section 8 engagement as follows: first, the collection of CEM by foreign agency partners, second, the Service's receipt of Processed CEM from a foreign agency partner and its subsequent use, and third, the Service's receipt of Bulk CEM and their subsequent use or exploitation in furthering an investigation pursuant to section 12 of the *CSIS Act*.

(1) The Collection of CEM by Foreign Agency Partners in the Course of their Conduct of Military Operations Abroad

[50] The evidentiary record before the Court demonstrates the CEM in issue was collected in foreign jurisdictions in the course of targeted operations undertaken by foreign coalition military forces.

[51] These circumstances differ from those in *Hape* in two principal respects. First, the coalition military forces involved in the collection of CEM are not necessarily engaged in, or undertaking, police investigations, but instead are involved in military operations that may

engage domestic and international legal frameworks beyond law enforcement. Second, certain of the coalition partners participating in the collection of CEM may be operating in third countries with or without the consent of the "host nation." While these distinctions are not unimportant, they do not alter the fact that the coalition forces involved in the collection of CEM are understood to be operating within their domestic legal frameworks and in accordance with their international legal obligations.

[52] Applying the *Hape* methodology, subsection 32(1) of the *Charter* is of no application because the conduct at issue – the collection of CEM – is not the conduct of a Canadian state actor. Rather, the CEM in issue has been collected by foreign coalition partners operating in a foreign state.

[53] Where the facts establish, as they do here, that the state activity in question does not fall under subsection 32(1) of the *Charter*, and recognizing that the fair trial exception to the non-application of the *Charter* does not arise in the context of a Service investigation, a court must then consider whether the information or evidence ought to be excluded on the basis that Service use of the information would cause Canada to be in violation of its international obligations in respect of human rights.

[54] The evidence before me does not suggest that the CEM shared with the Service has been collected in a manner that would cause Canada to be in violation of its international obligations. In this regard, inquiries were made and evidence received detailing the framework adopted by [...] to address the risk of mistreatment in the collection of CEM and the Service's obligations

under the *Avoiding Complicity in Mistreatment by Foreign Entities Act*, SC 2019, c 13, s 49.1. In issuing the warrants at the Phase 1 stage, I was satisfied the CEM collected by or on behalf of [...] was likely not the product of mistreatment.

[55] In written submissions, the *amicus* further submits that, pursuant to *Hape,* the *Charter* would generally not apply to the extraterritorial collection of CEM, even by Canadian actors. I note the *amicus*' view in this regard, but the issue of CEM collection by Canadian actors is not before the Court and I therefore express no opinion on this question.

[56] Having concluded the *Charter* is of no application to the collection of CEM by foreign agency partners, it follows that section 8 privacy interests cannot be engaged at the collection stage.

(2) The Service's Receipt and Use of Processed CEM

[57] The AGC and the *amicus* have advanced a single set of submissions on the question of *Charter* application to the Service's receipt of both Processed and Bulk CEM. However, I have considered the issues separately, and address *Charter* application to the receipt of Bulk CEM in the section that follows (see paragraphs 73–82).

[58] The AGC takes the position that receipt of CEM in either a Processed or Bulk form from its interagency partners, [...] does not engage the *Charter* because the information or material has already been obtained by a coalition partner in compliance with the foreign law governing

the conduct of that partner and that to then conclude the *Charter* applies at the point of sharing would be to indirectly apply the *Charter* extraterritorially to foreign agency conduct after the intrusion on any individual privacy interest has occurred. This outcome, the AGC submits, would not only be inconsistent with *Hape* but would be disconnected from the purpose of section 8 of the *Charter* – to balance state and private interests before state intrusion occurs and thereby prevent unjustified searches before they happen (*Hunter* at 160).

[59] The AGC acknowledges that the question of whether the receipt of information or material by the Service from its interagency partners engages the *Charter*, and more specifically section 8, has not been squarely addressed by this Court. However, in *Mahjoub (Re)*, 2013 FC 1093 [*Mahjoub*], Justice Edmond Blanchard did express the view that the sources of information relied upon to obtain warrants in that case included "information requested or supplied from other agencies in Canada and abroad" and that the sources relied upon were, if they engaged a reasonable expectation of privacy at all, minimally intrusive (*Mahjoub* at para 2; also see C-1-24 (2025 FC 1978) at paras 166–169 where Justice Kane addresses the Service's passive receipt of IP addresses).

[60] The *amicus* does not advance an opposing view on this issue.

[61] In the absence of jurisprudence in the national security context squarely addressing the application of the *Charter* to information or material received by the Service, the AGC has provided an extensive overview of the criminal law jurisprudence considering the issue in the

context of foreign law enforcement agencies sharing information with their Canadian counterparts.

[62] The AGC submits, and I agree, that the approach adopted in the criminal law context is of relevance and informs how this issue is addressed in the national security context.

[63] The AGC cites what it characterizes as "an unbroken line of cases" where courts at every level in a variety of contexts have held that the receipt of evidence from foreign law enforcement authorities relating to persons who have the benefit of protection under section 8, where the evidence was lawfully collected in the foreign jurisdiction, does not engage section 8 of the *Charter*.

[64] In the extradition context, the Supreme Court has held that section 8 does not apply to wiretap evidence shared with Canadian police authorities by US authorities who have collected the evidence in a manner that conforms with US domestic law but would have been unacceptable in Canada, even where Canadian police may have been cooperating with the foreign investigation (*United States of America v Dynar*, [1997] 2 SCR 462; *United States v Viscomi,* 2015 ONCA 484 at paras 47–48). Similarly, the sharing of information by Canadian authorities with a foreign law enforcement agency for extradition purposes has also been found not to be a search, but rather a communication of information that has been previously acquired (*Wakeling v United States of America*, 2014 SCC 72 at para 34 [*Wakeling*]). Whether evidence collection by Canadian authorities in extradition matters has to comply with Canadian legal standards is a

question that is governed by the location of collection (*United States v Ebanks*, 2019 ONCA 390 at para 7).

[65] In domestic criminal prosecutions, the jurisprudence has similarly consistently held that evidence gathered by foreign investigators in advancing a foreign investigation pursuant to the foreign law of application is not subject to the *Charter* even in circumstances where the subject of the Canadian prosecution was in Canada at the time the foreign agency collected the evidence in issue (*R v Della Penna*, 2012 BCCA 3 at paras 44–48 [*Della Penna*]).

[66] That Canadian police authorities are engaged in a cooperative investigation with foreign law enforcement agencies does not alter this principle; the foreign gathered and subsequently shared evidence, even when shared in near real time, is not subject to the *Charter* so long as the foreign police are not acting as agents of the Canadian police and the manner employed to gather the evidence would not render the trial unfair (*R v Mehan*, 2017 BCCA 21 at para 54 [*Mehan*]; also see *R v Nguyen*, 2016 BCSC 2181 at paras 29–36 [*Nguyen*]).

[67] With respect to information shared with Canadian authorities pursuant to the formal Mutual Legal Assistance Treaty process, the courts have again consistently found section 8 of the *Charter* is not engaged by the collection of the evidence outside of Canada, nor by the sharing of the evidence with Canadian authorities (*Schreiber* at paras 32–34; *R v F(JM)*, 2018 MBQB 156 at para 87).

[68] The jurisprudence identified above has consistently followed *Hape* in standing for the principle that the *Charter* is of no application to foreign investigative agencies. The jurisprudence further demonstrates that Canadian courts have consistently held the receipt of lawfully collected foreign information and its use in furtherance of a domestic criminal investigation by Canadian police authorities does not, subject to the limited exceptions identified in *Hape*, engage the *Charter* (*R v Calabretti*, 2021 BCPC 391 at para 18, citing *Mehan*, *Nguyen*, *Della Penna*, and *Wakeling*).

[69] Processed CEM is analogous to the type of shared evidence that has been judicially considered in the criminal law context – information has been collected by a foreign agency and then shared with Canadian authorities in either a raw form that may require some form of review to identify that which is pertinent to the investigation, for example unedited intercept transcripts, or in a processed form that is readily usable in furtherance of a domestic Canadian police investigation. This being so, I am satisfied that the *Charter* does not apply to the Service's receipt of Processed CEM from its foreign agency partners or its subsequent use.

[70] In summary, the jurisprudence supports the following:

a. The *Charter* does not apply to foreign agency collection of CEM – in a foreign jurisdiction in accordance with the foreign agency's governing legal framework – that is subsequently received by the Service as Processed CEM.

b. The Service's receipt of Processed CEM is not a search or seizure to which the *Charter* applies, but rather the communication of previously collected information.

This is so even where the Service would have required prior judicial authorization to directly obtain the same information.

c. The Service's use of Processed CEM subsequent to its receipt and in furtherance of an investigation similarly does not engage the *Charter*.

[71] I therefore agree with both the AGC and the *amicus* and conclude that the Service's receipt and use of Processed CEM in the circumstances disclosed by the evidence does not engage the *Charter*, and that the exceptions identified in *Hape* that might otherwise trigger the extraterritorial application of section 7 of the *Charter* are of no application.

[72] However, the jurisprudence relied on by the AGC does not expressly consider whether the receipt of an unexploited electronic device from a foreign partner and its retention by the Service, what is referred to as Bulk CEM in this matter, will trigger *Charter* application. The *amicus* argues that where the Service seeks to exploit lawfully collected Bulk CEM to further a domestic investigation, that the *Charter* may be of application and section 8 engaged. I now turn to these issues.

(3) The Service's Receipt and Use or Exploitation of Bulk CEM

[73] In *R v Vu*, 2013 SCC 60 [*Vu*], the Supreme Court recognized that, unlike traditional receptacles containing information obtained in the course of the authorized search of a place, electronic devices have the capacity of storing or providing access to vast amounts of information that may touch on an individual's biographical core of personal information. These

devices also automatically generate and retain information without a user's knowledge, may retain information a user believes has been destroyed, and, by way of network connections, may provide access to information well beyond that stored on the device (*Vu* at paras 40–45). The Court found that these markedly different privacy interests are potentially impacted where an electronic device is to be searched and therefore required that the search of a computer or electronic device be the subject of specific prior judicial authorization where the authorizing judge is able to balance privacy interests against the state's interest in intruding (*Vu* at paras 47–49).

[74] The Supreme Court has also recognized in *R v Marakah*, 2017 SCC 59 [*Marakah*] that third parties may have a reasonable expectation of privacy in the contents of another person's device. This is particularly so where what is sought in conducting the search of a device is the private electronic communications of that third party with the device owner (at paras 16–18).

[75] In short, *Vu* requires separate and distinct judicial authorization prior to the search of an electronic device and that search is, in turn, separate and distinct from the search of the place where the device may have been found. *Marakah* in turn recognizes the potential privacy interests of third parties in the electronic device of another person where that device contains information, including electronic communications of that third party, where the context discloses a third party's reasonable expectation of privacy in the information sought.

[76] *Vu* was decided in the context of a judicially authorized search of a place and the scope of reasons provided are restricted to the search of data stored on a computer found in those

circumstances (*Vu* at paras 63–64). However, the principles reflected in both *Vu* and *Marakah* have been recognized and applied in the national security context (*Sections 12 and 21 of the Canadian Security Intelligence Service Act*, 2019 FC 141 at paras 22–23).

[77] Recognizing the markedly different privacy interests that arise in the context of electronic devices, the courts have held that the handover of an electronic device by a third party to the police, unlike the handover of documents, may constitute a seizure by the police where the police take steps to assert control over the electronic device (*R v Lambert*, 2023 ONCA 689 at paras 59–61, 67 [*Lambert*]; *R v Reeves*, 2018 SCC 56 at paras 27, 56–58 [*Reeves*]; also see *R v Cole*, 2012 SCC 53 at para 65 [*Cole*]). The jurisprudence also distinguishes between the police receipt of information and the receipt of physical electronic evidence where retention of the electronic device may restrict access to that device (*Lambert* at paras 59–61; *R v Done*, 2025 ONCJ 326 at paras 60, 64–65). This line of jurisprudence highlights the potential distinction between the Service's receipt of Processed CEM, discussed above, and its receipt of Bulk CEM.

[78] The jurisprudence in the criminal law context establishes that the receipt and retention of an electronic device by Canadian authorities may engage section 8 of the *Charter* where the retention of the device will have the effect of restricting or depriving an individual with an ownership or control interest in the device from having access to that device.

[79] In this instance, the Service's receipt and retention of the Devices does not deprive an individual with an ownership or control interest in an electronic device from having access to that device. This is because the Service's Bulk CEM Holdings do not consist of original

electronic devices, but rather forensic copies or gold copies. The Service's receipt, retention, and control of Bulk CEM in this form cannot exclude the exercise of control over a device by an individual with an ownership or control interest, whether that individual is a section 8 rights-holder or not.

[80] In addition, any reasonable expectation of privacy that [...] may have in the Devices the Service seeks to exploit arises from the Service's belief that the Devices may contain [...] electronic communications with the Device owner. While *Marakah* teaches that [...] may retain a reasonable expectation of privacy in those communications, [...] privacy interest does not provide [...] with any ownership in or control over the Devices.

[81] These factors distinguish the Service's receipt and retention of electronic devices in the form of Bulk CEM from *Cole*, *Reeves* and *Lambert*.

[82] I am therefore satisfied that the Service's receipt and retention of the Devices specifically, and the Bulk CEM Holdings more broadly, does not engage section 8 of the *Charter*.

[83] Turning then to the Service's use or exploitation of Bulk CEM, the *amicus* submits that consideration of the question of *Charter* application must begin with a recognition that (1) the Service seeks to exploit Bulk CEM in the context of a domestic investigation of a person within Canada, (2) the Devices consist of forensic copies of electronic devices, and (3) individuals within Canada may retain a residual reasonable expectation of privacy in respect of the

information contained in Bulk CEM. The *amicus* also notes that [...], the subject of the Service investigation in this case, has been in Canada since [...].

[84] Citing *Vu*, *Marakah* and *Wakeling*, the *amicus* also submits that (1) Bulk CEM, consisting of electronic devices, attract a high expectation of privacy (*Vu* at paras 40–44), (2) the "zone of privacy" extends beyond a person's own electronic devices, and can include electronic conversations with others that are contained on another person's electronic device, and (3) although a reasonable expectation of privacy in communications found on another person's device is to be assessed in light of the totality of the relevant circumstances (*Marakah* at para 54), this expectation should be presumed in the national security context. This is because the Service's very objective in exploiting Bulk CEM is to obtain information that would implicate a person of interest's reasonable expectation of privacy, an expectation which persists following the initial lawful collection of a device (*Wakeling* at para 40).

[85] Relying on the above noted principles, the *amicus* argues that [...] has a residual privacy interest in the Devices the Service seeks to exploit, that this interest is sufficient to engage section 8, and that the exploitation of the Devices is more than minimally intrusive and therefore prior judicial authorization is required. In oral submissions, the *amicus* further argued that the Service's exploitation of the Devices in the context of furthering a domestic investigation is also properly characterized as a "new and different search" that directly implicates the section 8 analysis.

[86] The AGC submits in response that having concluded that the *Charter* has no application to either the collection or Service receipt of CEM, the *Charter* cannot logically be found to apply at the exploitation or analysis stage. To conclude otherwise would be to reject the "unbroken line of jurisprudence" arising in the "police to police" evidence-sharing context that holds neither the sharing of foreign gathered evidence with Canadian police nor the analysis or use of that evidence by Canadian police engages section 8 of the *Charter*. The AGC further submits that just as agency-to-agency sharing is not a new search as established in *Wakeling*, the subsequent exploitation of Bulk CEM that has been shared with the Service does not amount to a "new and different" search.

[87] Having carefully considered the submissions, I am of the view that the *Charter* does apply where the Service exploits Bulk CEM in furthering a domestic national security investigation involving a person who has a nexus to Canada.

[88] In light of *Vu*, I am respectfully of the opinion that the AGC's position – because the *Charter* had no application at the time of the collection or the Service's receipt of Bulk CEM, it cannot logically apply at the exploitation or analysis stage – fails to recognize the unique nature of electronic devices, that because of this unique nature the *Charter* may require judicial scrutiny and judicial authorization before an electronic device is exploited or searched, and that the search of an electronic device is separate and distinct from the search or actions that resulted in the seizure or obtaining of the device.

[89] Whether the *Charter* applies and section 8 is engaged where the Service undertakes a search of Bulk CEM is not to be determined, as the AGC argues, on the basis of the circumstances that prevailed at the time of collection or sharing. Instead, *Charter* application generally, and section 8 engagement specifically, must be considered in light of the totality of the circumstances at the time exploitation of Bulk CEM is proposed by Canadian authorities.

[90] The criminal law jurisprudence that the AGC relies upon to argue that in the "police to police" evidence-sharing context neither the sharing nor the analysis of shared evidence by Canadian police engages section 8 of the *Charter* is distinguishable. As noted above, none of the police-to-police sharing jurisprudence the AGC relies upon clearly involves the sharing of an unexploited electronic device that Canadian police then sought to independently exploit or search in furtherance of their investigation. That is what the Service seeks to do in this instance.

[91] The one exception is *McGregor*, a case involving the investigation of a member of the CAF serving in the US. Canadian military police authorities received electronic devices that had been seized by US authorities in the course of a search, authorized under US law, that Canadian authorities participated in. The military police subsequently sought a warrant prior to exploiting the devices in furtherance of their domestic investigation. On its face *McGregor* is supportive of the view that a warrant is required to search an unexploited electronic device provided by a foreign partner; however, this issue was never judicially considered. It is also important to note that *McGregor* arises in a context where the section 8 rights-holder, as a member of the CAF, remained subject to Canadian law while in the US.

[92] While directly analogous criminal jurisprudence has not been identified, the jurisprudence involving the police receipt of electronic devices from third parties demonstrates that police authorities are required to obtain a warrant prior to exploiting those devices.

[93] For example, in *Lambert*, where the accused's spouse voluntarily provided the police with two computers that contained suspected child pornography material and where the police wrongly believed a warrant was not required to retain the computers, the police nonetheless understood a warrant was required to access the data on the computers. The Court acknowledged the police action in properly obtaining a warrant prior to exploiting the seized computers (at para 43).

[94] I therefore conclude the *Charter* applies and section 8 is engaged where the Service seeks to exploit Bulk CEM in conducting an investigation involving a person with a nexus to Canada. I do not reach this conclusion on the basis that a residual privacy interest triggers the application of the *Charter*, but rather on the basis that (1) *Vu* requires prior judicial authorization before an electronic device is searched, (2) the prescribed search is a new or fresh search unconnected to the prior collection or receipt of Bulk CEM, and (3) the search is to be conducted within Canada by Canadian state actors in furtherance of a domestic national security investigation involving a person who has a nexus to Canada (*Charter*, s 32(1)).

[95] Having concluded section 8 is engaged where the Service seeks to exploit Bulk CEM in the conduct of a domestic investigation involving a person with a nexus to Canada, I will now

address the AGC's argument that the exploitation activity in this case may be undertaken without a warrant on the basis that it is a minimally intrusive form of search.

C. *Can the exploitation of the Devices be authorized without a warrant as a minimally intrusive form of search?*

[96] A search will be presumed to be unreasonable where it has not been preauthorized by a neutral and impartial arbiter capable of acting judicially. However, this presumption may be overcome where it is demonstrated that (1) the search is authorized by law, (2) the law is reasonable, and (3) the search will be carried out in a reasonable manner (*McGregor* at para 26).

[97] That the search of the Devices is authorized by section 12 of the *CSIS Act* and that the law is one that is reasonable is not disputed (see *Outside Canada* at paras 48–59). The AGC further argues that the search is minimally intrusive because, by engaging in electronic communications with foreign nationals outside Canada, [...] ran the risk of the electronic devices being seized and searched by foreign authorities and then shared with the Service. This, in the AGC's submission, lessens or limits [...] privacy interest in the Devices the Service seeks to search and thereby renders any warrantless search minimally intrusive and therefore reasonable.

[98] While I do not take issue with the principles underpinning the AGC's position, I am unpersuaded. This is because the argument fails to recognize that the search in issue, which involves electronic devices, is separate and distinct from the circumstances relating to the original collection or receipt of the Devices by the Service.

[99] The Service is not using information disclosed to it but is instead seeking to undertake an independent search of the Devices, a search that presumptively requires prior judicial consideration and authorization. The search would access the Device contents with the expectation that the Service will then obtain access to the contents of certain of [...]'s electronic communications, an intrusion on [...] reasonable expectation of privacy. These communications would in turn disclose information relating to [...] activities. This intrusion is more than minimal in nature and therefore the search requires prior judicial authorization (*Outside Canada* at paras 64–65).

.

D. *To what extent does the "dataset" regime in sections 11.01-11.25 of the* CSIS Act *apply to the Service's collection, analysis and retention of Bulk CEM Holdings under section 12 of the* CSIS Act*?*

[100] The Service holds [...] devices or gold copies that it has received as part of its routine sharing arrangement with [...]. This collection raises the question of whether the Service's Bulk CEM Holdings constitute a dataset and are subject to the dataset regime provided for in the *CSIS Act*.

[101] Following the Bill C-70 amendments to the dataset regime (Bill C-70, *An Act respecting countering foreign interference*, 1st sess, 44th parl, 2024 (assented to 20 June 2024), SC 2024, c 16), section 11.01 of the *CSIS Act* now defines a dataset as follows:

[…]	[…] :
dataset means a collection of information that	**ensemble de données** Ensemble d'informations qui, à la fois :
a) is characterized by a common subject matter;	**a)** porte sur un sujet commun;
b) is stored as an electronic record;	**b)** est sauvegardé sous la forme d'un fichier numérique;
c) contains *personal information* as defined in section 3 of the *Privacy Act*	**c)** contient des *renseignements personnels* au sens de l'article 3 de la *Loi sur la protection des renseignements personnels*;
d) is relevant to the performance of the Service's duties and functions under section 12 to 16 but cannot be collected or retained under any of those sections (*ensemble de données*)	**d)** est pertinent dans le cadre de l'exercice des fonctions qui sont conférées au Service en vertu de l'un des articles 12 à 16, mais ne peut être recueilli ou conservé au titre de l'un ou l'autre de ces articles. (*dataset*)

[102] "Dataset," as now defined, is limited to common subject matter information containing personal information relevant to the Service's duties and functions under sections 12 to 16 but which cannot be collected or retained under those authorities.

[103] The "dataset" definition results in the dataset regime only being engaged in those circumstances where the Service seeks to collect or retain information relevant to its section 12 to 16 duties and functions, but is not authorized to be collected or retained under sections 12 to 16. This definition ensures, recognizes, and coherently accommodates the meaning of a dataset

within the broader context of the *CSIS Act* which also establishes the Service's section 12 to 16 collection authorities. For example, in *Outside Canada*, Chief Justice Crampton held that the dataset regime would apply where the Service may seek to retain incidentally collected data pertaining to non-threat related parties (at para 117).

[104] In considering whether the Bulk CEM Holdings of the Service is subject to the dataset regime, it is first necessary to consider whether the Service is authorized to collect and retain this information under section 12 of the C*SIS Act.*

[105] The Service is authorized to collect and retain intelligence and information that is "strictly necessary… respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada…" (*CSIS Act*, s 12(1)).

[106] The Devices in issue were collected in the course of military operations targeting [...] violent extremists. It is the Bulk CEM collected in the course of these military operations against violent extremists that are [...] ultimately shared with the Service.

[107] There is much evidence to indicate the Devices the Service seeks authority to search in this Application may be retained under subsection 12(1). I am therefore satisfied that the subsection 12(1) "strictly necessary" requirement is met with respect to the Devices in issue. In so concluding, I recognize that the CEM shared with the Service will undoubtedly and unavoidably involve the incidental collection of non-threat-related information. This information, unless related to a threat to the security of Canada, is not authorized for retention

except where authorized pursuant to the dataset regime (*X (Re)*, 2016 FC 1105 at paras 197, 214).

[108] With respect to the remainder of the Service's Bulk CEM Holdings, the AGC has acknowledged in the course of oral submissions that there is little evidence in the record to establish the Bulk CEM Holdings may be retained under subsection 12(1). This being so, the AGC has also acknowledged that retention determinations are subject to the Service having assessed its Bulk CEM Holdings and only retaining the Bulk CEM assessed to be threat-related.

[109] On the basis of the above, I therefore conclude that the Bulk CEM Holdings assessed as threat-related are properly held pursuant to subsection 12(1) of the *CSIS Act* and are not subject to the CSIS dataset regime. Should the Service seek to retain Bulk CEM Holdings that are assessed as non-threat related, then the Service will be required to comply with the dataset regime and the timelines prescribed therein.

[110] With respect to the Bulk CEM Holdings that remain to be assessed, noting that in addition to the legal issues addressed in this decision there was some evidence that resource constraints were impacting the assessment of the Service's Bulk CEM Holdings, the Court will require the Service to report on the progress being made in assessing those Bulk CEM Holdings.

V. Conclusion

[111] In conclusion:

1. Pursuant to the *Hape* framework, the *Charter* does not apply to the collection of CEM by foreign agency partners in the course of their conduct of military operations abroad;

2. The *Charter* is not engaged by the Service's receipt of Processed or Bulk CEM from a foreign partner, nor the Service's use of Processed CEM;

3. The *Charter* applies, section 8 is engaged, and prior judicial authorization is required where the Service intends to search or exploit Bulk CEM in the conduct of a domestic investigation involving a person who has a nexus to Canada; and

4. Bulk CEM Holdings assessed as threat-related are not subject to the dataset regime set out at sections 11.01-11.25 of the *CSIS Act*.

ORDER IN CSIS 24-22

THIS COURT CONCLUDES AND ORDERS that:

1. The *Charter* does not apply to:
   a. foreign agency collection outside Canada of CEM that the Service receives as either Processed or Bulk CEM as part of interagency information sharing arrangements in furtherance of its mandate pursuant to section 12 of the *CSIS Act*;
   b. the Service's receipt of Processed or Bulk CEM;
   c. the Service's use of Processed CEM.
2. The *Charter* does apply and section 8 is engaged where the Service undertakes the search of Bulk CEM in furtherance of a domestic investigation involving a person who has a nexus to Canada.
3. The search of the Devices in furtherance of the Service's investigation in this case involves more than a minimally intrusive search and therefore requires that the Service obtain prior judicial authorization.
4. Any portion of the Service's Bulk CEM Holdings that has been assessed by the Service as threat-related and retained by the Service is not subject to the dataset regime as set out in sections 11.01-11.25 of the *CSIS Act*.
5. The Service shall provide the Court an update on the status of the assessment of its Bulk CEM Holdings not later than six months following the date of this Order.

"Patrick Gleeson"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CSIS 24-22
STYLE OF CAUSE:	IN THE MATTER OF AN APPLICATION BY [...] FOR WARRANTS PURSUANT TO SECTIONS 12 AND 21 OF THE CANADIAN SECURITY INTELLIGENCE SERVICE ACT, RSC 1985, c C-23 AND IN THE MATTER OF ISLAMIST TERRORISM AND [...]
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	JUNE 26 & 27, 2023 OCTOBER 15, 2024
CLASSIFIED ORDER AND REASONS:	GLEESON J.
DATED:	FEBRUARY 20, 2026

APPEARANCES:

Kendra Eyben Jeffrey G. Johnston Arlo Litman	FOR THE RESPONDENT
Matthew R. Gourlay	AMICUS CURIAE

SOLICITORS OF RECORD:

Attorney General of Canada Ottawa, Ontario	FOR THE RESPONDENT
Henein Hutchison Robitaille LLP Toronto, Ontario	AMICUS CURIAE