Federal Court  Cour fédérale

~~**TOP SECRET**~~

Date: 20240613

Docket: CSIS-20-21

Citation: 2022 FC 645

Ottawa, Ontario, June 13, 2024

PRESENT: The Honourable Mr. Justice Mosley

BETWEEN:

IN THE MATTER OF AN APPLICATION FOR JUDICIAL AUTHORIZATIONS PURSUANT TO SECTION 11.13 OF THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*, RSC 1985, c. C-23

AMENDED REASONS FOR JUDICIAL AUTHORIZATIONS

I. Introduction

[1] On November 23, 2021, an employee of the Canadian Security Intelligence Service [CSIS or the Service] applied in writing, and without notice to any other party, for judicial authorizations pursuant to section 11.13 of the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*] for the retention of two Canadian datasets for a period of two years. While there are differences between the two datasets, the context and the factors to satisfy the test for authorization are the same for both which is why they were combined in one application.

[2] The undersigned is a judge of the Federal Court designated by the Chief Justice thereof for the purposes of the *CSIS Act.* Upon being satisfied that the retention of the datasets ~~that~~ is likely to assist the Service in the performance of its duties or functions under sections 12, 12.1 and 16 of the *CSIS Act* and that the Service has complied with its obligations under section 11.1 with respect to the datasets, I authorized the retention of the datasets on March 10, 2022 with terms and conditions which I considered necessary or advisable in the public interest.

[3] These reasons for the issuance of the requested judicial authorizations are intended for public dissemination and have been written without reference to the personal information in question or the circumstances in which it was collected for privacy and national security reasons.

II. **Legislative context**

[4] This was the first application for judicial authorizations for the retention of datasets pursuant to section 11.13 since *An Act Respecting National Security Matters* SC c C-13 [*National Security Act* or *Bill C-59*] creating the dataset regime was assented to on June 21, 2019.

[5] The dataset amendments stemmed at least in part from the decision of Mr. Justice Simon Noël in *X (Re),* 2016 FC 1105 regarding the Service's illegal retention of data associated with lawfully collected communications. Justice Noël held that the *CSIS Act* authorizes the Service to collect and retain only that information which is "strictly necessary" to carry out its mandate. CSIS was, in effect, keeping such data even if it was not immediately threat-related in the event

that it might prove to be useful later on. Justice Noël acknowledged the intelligence value of data analysis and questioned whether the legislation governing the Service was keeping pace with technological developments.

[6] Among other extensive changes to the security and intelligence legislative framework, the *National Security Act* created a detailed and complex regime for the collection and retention of datasets containing personal information as that term is defined in section 3 of the *Privacy Act*, RSC, 1985, c P-21. This regime can be seen as Parliament's response to Justice Noël's questions about the adequacy of the legislation.

[7] Section 3 of the *Privacy Act*~~, which is set out in Annex "A" to these reasons,~~ defines personal information very broadly as information about an identifiable individual that is recorded in any form. It includes information about race and ethnicity, religion, age or marital status, education, criminal or employment history, identifying numbers assigned to the individual, the personal views or opinions and correspondence of a private or confidential nature of the individual. What is not included in the meaning of personal information is also set out in s 3 of the *Privacy Act.* For the purposes of this application, the contents of the datasets in question clearly constitute personal information.

[8] "Dataset" is defined in section 2 of the *CSIS Act* to mean "a collection of information stored as an electronic record and characterized by a common subject matter". The governing provisions regarding the collection and retention of datasets pertaining to information not

collected under the authority of a judicial warrant are set out in sections 11.01 to 11.25, 27 and 27.1 of the *CSIS Act* ~~and are reproduced in Annex "B" to these reasons~~.

[9] The new regime applies only to datasets that contain personal information and which do not directly and immediately relate to activities that represent a threat to the security of Canada. The information would not therefore fall within CSIS's s 12 mandate. Its collection by the Service, however, would likely constitute a search or seizure invoking section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 11982, c11I. Retention and exploitation of the information by CSIS would also be problematic. Hence the need for the elaborate scheme enacted by Parliament including the authorizations for retention of datasets from an independent and neutral judicial arbiter which are the subject of these reasons.

[10] The scheme distinguishes between datasets which relate to publicly available information, information which predominantly concerns Canadians or persons within Canada, and that which predominantly relates to non-Canadians outside Canada. CSIS must be satisfied that the dataset is relevant to the performance of its duties and functions under the Act. Should the dataset relate to Canadians or persons within Canada it must fall within a preapproved class of datasets authorized for collection by the Minister of Public Safety and which have been approved as reasonable by the Intelligence Commissioner.

[11] The approved classes of datasets have not been made public but the decisions by the Minister and the Intelligence Commissioner were included as exhibits to the Applicant's affidavit. They are exceptionally broad in scope and I had no difficulty accepting that the datasets in question in this application fell within them. Indeed it is difficult to see how any collection of personal information might be excluded given the breadth of their scope.

[12] For 90 days following the acquisition of the dataset or until an authorization to retain is sought and approved, the Service cannot query the information for intelligence purposes except in exigent circumstances where life, individual safety, or perishable information of significant value to national security is at risk of being lost. They may review the information to determine what it consists of and whether it would be useful to an ongoing investigation and to prepare any applications that may be required. During this period, and for so long as the Service retains the dataset, it is required to delete any information related to a person's mental or physical health in which there is a reasonable expectation of privacy, and information that is subject to solicitor-client privilege.

[13] To retain a Canadian dataset for longer than 90 days, CSIS must obtain, with the Minister's approval, judicial authorization from the Federal Court. To retain a foreign dataset beyond that timeframe, they must obtain the Minister's authorization. The decision to retain a foreign dataset is reviewed on reasonableness grounds by the Intelligence Commissioner.

[14] These reasons pertain only to the two Canadian datasets which are the subject of the application. Under the legislation, the Court must be satisfied that the dataset is likely to assist CSIS in the performance of its security and foreign intelligence and threat reduction duties and functions. The Court may impose any terms and conditions on the retention and use of a dataset that it considers advisable in the public interest. The duration of the authorization is for up to two years, subject to renewal. During that period, CSIS may conduct specific searches of the dataset relating to a person or entity, which is known as a "query". They may also conduct an "exploitation", which means a computational analysis of the dataset to obtain intelligence not otherwise apparent. These operations must be strictly necessary to CSIS's security intelligence and threat reduction mandates under ss 12 and 12.1 of the Act or required for its foreign intelligence function under s 16.

[15] The datasets must be kept separate and apart from the Service's other operational collections. Access to them is only permitted to persons specially designated by the CSIS Director. Should a query or exploitation provide information of intelligence value the retention of which is determined to be strictly necessary, a designated person can transfer the results to the operational side of the Service's data collections where it can be used for investigative purposes. Otherwise it must be destroyed.

[16] The legislative scheme also calls for periodic and random auditing and the reports generated by the audits must be provided to the National Security and Intelligence Review Agency (NSIRA). Section 27.1 of the *CSIS Act* empowers NSIRA to report to the Director, who

is, as soon as feasible, to convey the report to the Court, on dataset activity that may not be in compliance with the law. A Designated Judge of the Court shall review the information and make a determination if the querying or exploitation by the Service complied with the law and may make any order or take any other measure that the judge considers appropriate in the circumstances.

[17] This provision in the legislation provides a means for the review agency to make its views known to the Court. Such disclosure was not previously possible other than through the publication of the review agency's non-classified annual reports. Those public reports are necessarily vague, for national security reasons. This change in the law will assist the Court to better understand how its orders are executed by the Service, at least in this one aspect of the legislation.

[18] While not directly pertinent to this application, I note that in so far as information is collected incidentally in relation to a threat to the security of Canada under the authority of a warrant issued by the Court, section 21 (1.1) now provides that the applicant for a warrant may ask the judge to authorize the retention of the information in order to constitute a dataset.

[19] Section 28 of the *CSIS Act* was also amended by Bill C-59 to provide that the Governor in Council may make regulations prescribing the form of judicial authorizations that may be issued under section 11.13 and for governing the practice and procedure of, and security

requirements applicable to, hearings of applications for judicial authorization under section 11.13.

III. **Procedural History**

[20] At the time of writing, no regulations have been made with respect to these matters. Accordingly, the procedure followed was similar to that employed in dealing with applications for the issuance of warrants under the *CSIS Act* and proceedings under related statutes. A Notice of Application was filed in the Designated Proceedings Registry on November 23, 2021 and a Top Secret file was opened by the Registry. The Applicant, represented by counsel from the National Security Litigation and Advisory Group [NSLAG or AGC counsel] of the Department of Justice, affirmed an affidavit in support of the application and draft authorizations for the Court's consideration with the Notice of Application.

[21] As this was a novel proceeding, a highly experienced security cleared counsel from the private bar, Mr. Gordon Cameron, was appointed as *amicus curiae*. The *amicus* had access to all of the material submitted to the Court and attended the *in camera* hearings.

[22] Following an initial review of the affidavit and draft authorizations, the Court convened a case management conference with NSLAG counsel and the *amicus* on November 30, 2021 to discuss the next steps.

[23] At the Court's request, a copy of the Director's authorization to permit queries of the datasets in exigent circumstances was provided as well as the Intelligence Commissioner's decisions and reasons approving the Director's authorization. Pursuant to subparagraph 11.13(2)(f), the application must set out the content of the Director's authorization. This was done in the affidavit filed in support of the application. It would be preferable, in my view, for the actual authorization to be provided in any future applications in order for the Court to be satisfied that this legislative requirement has been met.

[24] The initial affidavit filed in support of the application contained information current to November 17, 2021. To update that information, a supplemental affidavit was made by the same affiant on December 14, 2021 and was filed on December 15, 2021.

[25] Hearings took place on December 15 and 17, 2021. On those dates, the affiant appeared and was questioned under oath by NSLAG counsel, the *amicus* and the Court. An exhibit prepared by the affiant for illustrative purposes to explain the tables in which the information had been received by the Service was filed during the hearing. In addressing the Court at the outset of the hearings, AGC counsel made a statement recognizing her obligation as an officer of the Court, particularly in *ex parte* applications such as this, to ensure that no information adverse to the interests of the Service had been withheld from the Court. She also recognized her obligation to act independently of the Service, to maintain her objectivity and to advise the Court of all relevant legal considerations that arise in the context of the matter.

[26] The affiant's first affidavit contains a paragraph which similarly recognizes the duty of candour on the part of Service employees providing information and evidence to the Court. This was also addressed at the beginning of the affiant's direct examination by AGC counsel. The affiant stated that she understood her obligation was to provide full, frank and fair disclosure to the Court and that the obligation extended to other members of the Service who had provided information to her, such as the operational personnel who had handled the datasets. She had explained that obligation to the other Service members and received assurances that they understood the duty.

[27] Statements of this nature have been adopted as policies by both the Service and the AGC as a result of concerns expressed by the Court in several other matters in which the Court had found that the information provided in applications for warrants was incomplete and that material facts had been withheld. The Court has no reason to believe that to be the case in this instance. However, as became apparent during the Applicant's cross-examination, the information provided about the sources of information relied upon in support of the application was lacking in certain specificity. This did not, in the Court's view, reflect a deliberate attempt to withhold material facts but rather uncertainty as to what would be required to justify the application.

[28] The Applicant also averred that she had made the necessary inquiries and, to the best of her knowledge and belief, no information contained in her affidavit had been obtained through

the use of torture or other cruel, inhumane or degrading methods. She reiterated this declaration in her testimony and was cross-examined on the basis for this assertion.

[29] In addition to these specific subjects, the Applicant was closely questioned on the sources of the information collected by CSIS, how it was assembled and managed and how retention of the data bases would assist the Service in the performance of its duties.

[30] As described in her initial affidavit and testimony, the Applicant's Service experience is primarily as a data exploitation analyst. She has had a role in the Service as a subject-matter expert regarding datasets. Her position is situated within the Data Management and Exploitation Branch of the Service (DMEX) which includes the Operational Data Analysis Centre (ODAC). Her unit, Data Acquisition and Governance (DAG), is part of ODAC and provides advice both to ODAC and across the Service with respect to datasets.

[31] As a result, the affiant has been designated in accordance with s 11.07 of the *CSIS Act* for the purpose of conducting evaluation activities on datasets. These activities include the evaluation of datasets to determine if they fall within the regime and translation or decryption if necessary. This is done with a view to prepare the dataset, if appropriate, for an application for retention. During the evaluation period, the dataset may not be queried or exploited. It may be consulted for evaluation purposes.

[32] The affiant testified that she was the designated employee who consulted and evaluated the two datasets in question. In her affidavits and testimony she described how the datasets initially came to the attention of the Service and how they were collected through requests from the Service to other Government of Canada departments and agencies. She described the interaction between the Service and those departments and agencies. Some information in the datasets was initially provided by a foreign agency. The information in total comprised 26 spread sheets arranged in columns with different headings relating to subject matter which could be construed as personal information.

[33] When the information was obtained by CSIS, it was compared to the Service's operational holdings. It had initially been acquired under the *CSIS Act* s 12 mandate to collect, "…to the extent that it is strictly necessary, analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada…".

[34] In the circumstances in which the information had been obtained, it had been considered by the Service that it was "strictly necessary" to collect the information under its s 12 mandate in order to assess whether it related to persons who constituted a threat to the security of Canada. On the evidence presented to the Court, that was a reasonable conclusion. The question arose as to what to do with the information, which is not itself threat-related, in light of other threat-related information that came to the attention of the Service at the same time.

[35] The decision was taken to invoke the dataset regime and to request approval to query the information under the exigent circumstances provision in s 11.22 of the Act. This was authorized by the Director and that decision was subsequently validated by the Intelligence Commissioner as required by s 11.23.

[36] Following the exigent circumstances review, the information was turned over to the Applicant. The spreadsheets in question contained rows of data elements in columns pertaining to the subject individuals. The witness reviewed the contents of the tables to determine whether any of it appeared to contain medical or mental health information or solicitor-client information that would require destruction. The spreadsheets, in which the information was originally received by email and disseminated within the Service, were destroyed. The Applicant testified that those Service employees who had received the information confirmed its destruction once it was determined that it would fall within the dataset regime and retained only if it were to be determined to be strictly necessary and authorized by the Court.

[37] The information is now retained in a separate location from other Service data holdings and access to the information is limited to designated persons and access for queries or exploitation requested by other branches of the Service is recorded and can only be done if strictly necessary to assist the Service in the performance of its duties under ss 12 and 12.1 of the Act or to assist the Minister of National Defence or Minister of Foreign Affairs under s 16 of the Act.

[38] In her testimony, the Applicant took the Court through the tables and explained how the information was organized and described her findings from reviewing the content. In particular, she explained how she was able to determine that the information related to Canadians or persons in Canada and how it fell within one of the classes of datasets approved by the Minister and Intelligence Commissioner.

[39] The Applicant testified as to the need to update the tables should new information be received that affected any of the data elements while the dataset was retained.

[40] At the conclusion of the Applicant's testimony, counsel and the *amicus* provided the Court with oral submissions with respect to the merits of the application and the proposed authorizations. The *amicus* proposed additional language for insertion as conditions in the draft authorizations for the Court's consideration and a possible caveat to be attached to the data in the Service collection. The text of the proposed conditions and the caveat had previously been shared with AGC counsel but no consensus had been reached regarding their inclusion.

[41] Following receipt of the submissions, the Court indicated that the authorizations would not be issued in the draft forms submitted by the Applicant. AGC counsel and the *amicus* were directed to confer on changes to the proposed text in accordance with the Court's expressed concerns. Of particular concern to the Court were the proposals by the Service on how the datasets might be updated and edited by additions, deletions and corrections on an ongoing basis. It appeared that the Service sought *carte blanche* to revise the database without further

authorization from the Court. Also of concern was that, as originally proposed, the information could be queried or exploited without reference to the particular context in which it had been collected. This could have implications for the privacy interests of the individuals concerned, particularly if the information was to be shared with foreign agencies.

[42] On December 21, 2021 AGC counsel submitted a letter requesting additional time in which to respond with new text and written representations. The Court agreed to the proposed schedule and it was further extended at the request of the AGC. Additional evidence and submissions were submitted to the Court on February 9, 2022 to address the Court's concerns and proposals made by the *amicus* for additional terms and conditions. At the Court's direction, counsel for the AGC and the *amicus* continued to confer in an effort to arrive at a joint position to present for the Court's consideration. This process was prolonged by the difficulties presented by the pandemic. Given the subject matter, discussions between AGC counsel and the *amicus* could not be conducted outside the Court's secure facility.

[43] The AGC submitted revised draft authorizations on March 4, 2022 indicating where the proposed changes reflected a joint position with the *amicus.* The *amicus* provided a separate communication to the Court to explain his views on the revisions and to bring some further matters to the Court's attention.

[44] The *amicus* had previously recommended that an additional condition be included to require periodic reporting to the Court on queries and exploitation of the datasets. This was

intended to address a concern about possible inappropriate migration of the information to the Service's general s 12 operational databases. The AGC opposed this proposal on the grounds that it was unnecessary and duplicative of the work of NSIRA which would be reviewing the Service's use of the datasets as described above.

[45] The Court agreed with the AGC that, in this instance, it was not necessary or conducive to judicial economy to require routine reporting to the Court when the NSIRA review process was likely to be more efficient and effective. The Court is not in as good a position to monitor the risk of inappropriate migration as the review agency and is confident that NSIRA will be alert to the possibility. And could bring any misuse of the authorizations to the Court's attention. This conclusion, while general in nature, is also dependent on the facts of these applications and may need to be revisited in another matter.

[46] The revised draft authorizations limit the scope of the definition of the datasets and specify that they may only be updated in accordance with the terms of the authorizations. Those terms include two conditions. The first condition requires the Service to notify the Court of any determination that an update, other than an update pertaining to contact information, is to be made and places a hold on the update should the Court require further information or submissions regarding the proposed change.

[47] The second condition requires that a text be applied to any report querying or exploiting the dataset which describes the context in which the dataset was obtained including the

circumstances of the individuals to whom the information pertains. This was in response to a proposal by the *amicus* that a caveat be included in any Service reporting of the information. The Court was satisfied that the addition of the text would ensure that there was no confusion about the nature and source of the information that could lead to inappropriate consequences for the individuals concerned.

IV. **Outcome**

[48] As required by the statute, I was satisfied that the statutory formal prerequisites for the issuance of the authorizations were observed. These include designation of the Applicant by the Minister of Public Safety and Emergency Preparedness for the purposes of the applications, that the Deputy Minister had been consulted and that the Minister had personally approved the applications.

[49] Based on the Applicant's affidavit evidence and her testimony before the Court, and as required by subsection 11.13(1) of the *CSIS Act,* I am satisfied that retention of the datasets is likely to assist the Service in the performance of its duties or function under sections 12, 12.1 and 16 of the *CSIS Act* and that the Service has complied with its obligations under section 11.1 of the *Act.* I am satisfied that the matters referred to in paragraphs 11.13(2) (a) to (f) of the *CSIS Act* are supported by the evidence received by the Court.

[50] I therefore authorized the retention of the datasets by the Service for a period of 2 years from the date of issuance of the Order, March 10, 2022, and authorized the datasets to be updated in accordance with the terms and conditions of the Order.

[51] These were novel applications and the Court wishes to thank counsel for the AGC and the *amicus* for their assistance to the Court in dealing with them. The Applicant is also to be commended for giving her evidence in a clear and forthright manner.

[52] In addition to his submissions on the substantive merits of the applications, the *amicus* made some valuable suggestions about the form of the affidavit evidence tendered by the Service and the manner in which other Service personnel had been consulted in preparation of the application. These suggestions of a more general nature about the process will be shared with all Designated Judges for their consideration in respect of other applications for warrants and authorizations.

"Richard G. Mosley"

Judge

~~**TOP SECRET**~~

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	CSIS-20-21
STYLE OF CAUSE:	IN THE MATTER OF AN APPLICATION FOR JUDICIAL AUTHORIZATIONS PURSUANT TO SECTION 11.13 OF THE CANADIAN SECURITY INTELLIGENCE SERVICE ACT, RSC 1985, c. C-23
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	NOVEMBER 30, 2021 DECEMBER 15, 2021 DECEMBER 17, 2021
AMENDED JUDGMENT AND REASONS:	MOSLEY J.
DATED:	JUNE 12, 2023
AMENDED JUDGMENT AND REASONS:	MOSLEY J.
DATED:	JUNE 13, 2024

APPEARANCES:

Proja Filipovich Kendra Eyben	FOR THE APPLICANT
Gordon Cameron	*AMICUS CURIAE*

SOLICITORS OF RECORD:

Attorney General of Canada Ottawa, ON	FOR THE APPLICANT
Gordon Cameron Ottawa, ON	*AMICUS CURIAE*