Canadian Human Rights Tribunal

Tribunal canadien des droits de la personne

Citation: 2025 CHRT 79
Date: August 11, 2025
File No.: HR-DP-2972-23

Between:

CB

Complainant

- and -

Canadian Human Rights Commission

Commission

- and -

CANADIAN SECURITY INTELLIGENCE SERVICE

Respondent

Ruling

Member: Athanasios Hadjis

[1] The Complainant alleges in her complaint that she was discriminated against while employed by the Respondent, the Canadian Security Intelligence Service (CSIS). In an earlier ruling (*CB v. Canadian Security Intelligence Service*, 2024 CHRT 27 (the "First Ruling")), I issued a confidentiality order that included a direction that the Complainant only be identified by the random initials CB.

[2] The hearing into the complaint is scheduled to begin in about a month, on September 8, 2025. The Respondent has requested an additional confidentiality order expanding the scope of the existing order and addressing how the hearing is conducted. The Complainant takes no position on the request. As the Canadian Human Rights Commission has recently advised the Tribunal that it is no longer participating in the Tribunal's process regarding this complaint, it did not participate in this motion.

[3] For the following reasons, I grant the order but subject to certain conditions.

CSIS'S REQUEST

[4] My first ruling consisted basically of the following:

1) The Complainant would be identified as CB in all facets of the case, including any documents and pleadings filed with the Tribunal.

2) The name of any current or past CSIS employee who was or is likely to become engaged in covert CSIS operational activities (i.e., as described in s. 18(1) of the *Canadian Security Intelligence Service Act*, R.S.C., 1985. c. C-23 (the "CSIS Act")) would also be identified by random initials or a pseudonym.

3) A methodology was set out to enable the Complainant to learn the identity of such an employee where the information available to them is insufficient to identify them and their involvement in the case, while still preserving that information's confidentiality.

[5] CSIS wishes to expand the order to encompass information that it claims would be subject to “national security privilege”, consisting of the following information referred to in s. 38 of the *Canada Evidence Act*, R.S.C., 1985, c. C-5:

> “potentially injurious information”: information of a type that, if it were disclosed to the public, could injure international relations or national defence or national security.
>
> “sensitive information”: information relating to international relations or national defence or national security that is in the possession of the Government of Canada, whether originating from inside or outside Canada, and is of a type that the Government of Canada is taking measures to safeguard.

[6] I will refer to this information in this ruling as “Confidential Information”.

[7] CSIS states that the Confidential Information that may emerge in the context of CB’s case and hearing would be information that would identify or tend to identify:

1) employees, internal procedures and administrative methodologies, and telecommunications systems used by CSIS;

2) methods of operation and investigative techniques utilized by CSIS;

3) relationships that CSIS maintains with foreign police, security and intelligence agencies, and information exchanged in confidence with such agencies;

4) CSIS’s interest in individuals, groups, or issues, including the existence or nonexistence of past or present files or investigations, the intensity of investigations, or the degree or lack of success of investigations; and

5) individuals who provided information to CSIS.

[8] Thus, the requested confidentiality order would not just cover the identities of the employees referred to in the First Ruling but also other information, including CSIS

employees who do not have any past, present, or anticipated future involvement in covert activities (s. 18(1) of the CSIS Act).

[9] CSIS filed an affidavit signed under a pseudonym by a person employed at CSIS as an intelligence officer since 2004 (the “Affiant”). The Affiant explained that generally only the identities of CSIS’s Executive Committee are publicly available. Even the identities of persons not involved or likely to be involved in covert activities are potentially valuable to actors engaged in threat-related activities, including activities unrelated to terrorism. If the employee’s identity becomes known, such actors could identify the employee’s vulnerabilities and seek to exploit them.

[10] The affidavit sets out several examples in the past where the health and well-being of these types of employees or their families was put at risk. The affidavit also notes that even if an employee is not engaged in any covert activity, disclosure of their identities may prejudice their ability to be employed in a covert capacity in the future. Disclosure of these non-covert activity employees may also result in the identities of covert-activity employees being inadvertently disclosed if the two groups are seen engaging socially outside the office.

[11] Aside from the identities of all CSIS employees, the Affiant explains why other information encompassed in the Confidential Information must be protected from disclosure.

[12] The sustained collection of internal procedures and administrative methods over time could reveal how CSIS manages its investigations, how messages are generated and to whom they are sent, and how file numbers are used to distinguish between targets, sources of information, investigations, and the geographical area where investigations are conducted. Given the capacity of modern data analytics, these seemingly innocuous pieces of information are valuable to those whose activities threaten Canada’s national security and must continue to be protected from disclosure.

[13] CSIS uses secure telecommunication facilities or cryptographic systems to transmit information. The disclosure of security intelligence reports or information containing details that could identify these systems could compromise them.

[14] CSIS also uses specific methods in its security intelligence operations. The disclosure of such information would reveal the capabilities as well as the limitations of CSIS's methods and the degree of expertise possessed by CSIS. Similarly, the disclosure of information that would identify or assist in identifying CSIS's methods of operation would assist current and future subjects of investigation to counter CSIS's efforts. In addition, disclosure of the use of an investigative technique would seriously prejudice the efficacy of any future use of this technique.

[15] CSIS also cooperates with multiple foreign agencies. Trust and confidence in the ability of CSIS to protect information is essential to the relationships CSIS has established under s. 17 of the CSIS Act with foreign agencies. CSIS and foreign agencies share information with the express or implicit understanding that neither the information nor its source will be disclosed without the prior consent of the entity that provided it.

[16] Furthermore, the Affiant states that information identifying CSIS's interest in individuals, groups or issues, including the existence or non-existence of past or present files or investigations, the intensity of investigations, or the degree or lack of success of investigations, would prevent CSIS from operating effectively.

[17] The Affiant also noted that a number of individuals collaborate with CSIS by providing information that is valuable to its investigations and the national security of Canada. It is important for CSIS to protect the identities of these individuals to ensure their safety, to continue to have access to the information they provide, and to encourage others to collaborate with CSIS.

[18] For all these reasons, CSIS asks that Confidential Information be redacted from any documents filed in this case, including the identity of any CSIS employee, not just those referred to in the First Ruling.

[19] Furthermore, in order to protect the identities of any CSIS employee who may be testifying at the hearing, CSIS is requesting that their faces not be "displayed" in any public proceeding by ensuring that the testimony of current or past CSIS employees, including the Complainant, be *in camera*. Current or past CSIS employees would testify via videoconference with their camera turned on. CSIS is not requesting that the Complainant

necessarily testify by video, however. Only the Tribunal member, necessary Tribunal staff, the Complainant and her counsel, CSIS's representatives and counsel, and the Commission's representatives and counsel would be present during the testimony of any current or past CSIS employees.

[20] Following the testimony of current or past CSIS employees, CSIS would receive the audio recording and CSIS would be granted time to review the audio for Confidential Information. CSIS would redact any Confidential Information prior to the release of the audio recording to the other parties and the public.

[21] CSIS also requests that before the Tribunal releases any written ruling or decision in this matter, CSIS and the Complainant's counsel would be provided with a copy of the decision that is final, pending any redactions. CSIS counsel would advise the Tribunal if any Confidential Information for redaction is identified prior to the release of the decision to the public or the parties. If redactions for Confidential Information are identified, the redacted version of the decision will be placed into the official record and the original decision will be marked as confidential and not part of the publicly accessible record.

ANALYSIS

[22] Section 52(1) of the *Canadian Human Rights Act*, R.S.C., 1985, c. H-6 (CHRA) states that Tribunal inquiries are conducted in public. This reflects the principle that hearing processes should be held in the open. As the Supreme Court of Canada stated in *Sherman Estate v. Donovan*, 2021 SCC 25 at para 1 [*Sherman Estate*], the open court principle is protected by the constitutionally entrenched right of freedom of expression and, as such, it represents a central feature of a liberal democracy.

[23] However, exceptional circumstances do arise where competing interests justify a restriction to the open court principle (*Sherman Estate* at para 3). Thus, in the present context, under s. 52(1)(a) of the CHRA, Tribunal members may take any measures and make any order to ensure their confidentiality of an inquiry if they are satisfied there is a real and substantial risk that matters involving public security will be disclosed.

[24] As I noted in the First Ruling at paragraph 6, the person asking the Tribunal to exercise its discretion and to issue such an order must establish that:

1) Court openness poses a serous risk to an important public interest;

2) The order sought is necessary to prevent this serious risk to the identified interest because reasonable alternative measures will not prevent this risk; and

3) As a matter of proportionality, the benefits of the order outweigh its negative effects.

[25] Based on the information in the affidavit, I am satisfied that there is a real and substantial risk that if the Confidential Information is allowed to be revealed, matters involving public security will be disclosed (s. 52(1) of the CHRA).

[26] The least intrusive measure to protect this public interest is to hold the hearing *in camera* and not publicly release any Confidential Information. The Complainant will be able to fully participate at the hearing and will continue to be able to know the identity of the individuals referred to during the course of the hearing. The Complainant will not be impeded from pursuing her complaint. The hearing's recording will eventually be made public once it has been vetted for any Confidential Information.

[27] However, I do not agree with CSIS's request that it be permitted to unilaterally determine which portions of the rulings, decision and audio recordings must be redacted from public access. The Tribunal will review CSIS's proposed redactions, and if the Tribunal rejects any of proposed redactions, it will notify the parties of this determination at least one week before providing public access to the material.

[28] Finally, regarding the third element of the test, I find this important need to protect national security activities outweighs the negative effects arising from the redaction of the Confidential Information. In any event, this information is unlikely to be relevant to the human rights issues raised in the Complainant's complaint, as is perhaps evidenced by the Complainant's decision not to take a position on CSIS's request.

[29] I therefore find that the three parts of the test have been met and that, in accordance with the Tribunal's authority under s. 52 of the CHRA, a confidentiality order should be granted with the conditions set out below.

[30] The hearing has been scheduled to occur in person at the Tribunal's hearing rooms in Ottawa, starting September 8, 2025. Given that practically all of the testimonies are now set to be presented by video, it does not seem necessary to hold the hearing in person. I therefore propose that the hearing be conducted entirely by video. However, I am prepared to hold some or all of the hearing in-person with a video feed (i.e., hybrid format) if the parties prefer. The parties are requested to inform the Tribunal by August 15, 2025, if they are opposed to holding the hearing by video only.

ORDER

[31] For these reasons, I replace the order issued in the First Ruling with the following new order pursuant to s. 52(1)(b) of the CHRA:

1) Any sensitive or potentially injurious information within the meaning of s. 38 of the Canada Evidence Act, including information identifying the Complainant or any current or past CSIS employee, is designated "Confidential Information".

2) Any documents containing Confidential Information must be redacted to remove the Confidential Information, and only redacted versions may be filed with the Tribunal. For documents already in the Tribunal record that contain Confidential Information, the new redacted versions will replace the old versions. Once replaced, the parties who received the document and the Tribunal will destroy the old unredacted versions.

3) Any current or past CSIS employee must be identified solely by consistent random initials or other pseudonyms in all documents and pleadings filed with the Tribunal.

4) At the request of the Complainant, the full name of a current or past CSIS employee must be disclosed to the Complainant where the position title and other provided information alone are insufficient to identify who the employee is and their involvement in an issue. Such disclosure must occur either before the hearing, in direct communication between the parties, or during an in-camera portion of the hearing. The Tribunal and the parties must keep the information in confidence and cannot publicize it nor include it with any documentation submitted to the Tribunal.

5) All parties must respect the confidentiality of the Confidential Information by not referring to any Confidential Information publicly or in any public proceeding and by only referring to current or past CSIS employees by the random initials or other pseudonyms assigned to them. During the hearing, Confidential Information may only be referred to during in-camera sessions.

6) During the hearing, current or past CSIS employees will not display their face in any public (i.e., non-in camera) proceeding.

7) The testimony of current or past CSIS employees, including the Complainant, will be in camera. Current or past CSIS employees, including the Complainant, will testify via videoconference with their video camera turned on. Only the Tribunal member, necessary Tribunal staff, the Complainant and her counsel, and CSIS's

representatives and counsel will be present during the testimony of any current or past CSIS employees. Following the testimony of current or past CSIS employees, the parties will receive the audio recording of the hearing and be granted time to review the audio for Confidential Information. CSIS may, within two weeks of receiving the recording, propose the redaction of any Confidential Information that it may find on the recording, which will not, in the meantime, be available for public access. The Tribunal will review CSIS's proposed redactions and if the Tribunal rejects any of them, it will notify the parties of this determination at least one week before providing public access to the recording. The Tribunal will redact any necessary portions from the audio recording for the purposes of the publicly accessible official record. The original unredacted recording will be marked as confidential and not form part of the publicly accessible official record.

8) Before the release of any written ruling or decision by the Tribunal in this matter, counsel for CSIS and the Complainant will be provided with a copy of the ruling or decision that is final, pending any redactions. Within two business days after receiving the copy, or such other time specified by the Tribunal in consultation with the parties, CSIS's counsel will advise the Tribunal if they have identified any Confidential Information for redaction prior to the release of the ruling or decision to the public. If redactions for Confidential Information are identified and approved by the Tribunal, the redacted version of the decision or ruling will be placed into the official record and the original decision will be marked as confidential and not form part of the publicly accessible official record. If the

Tribunal rejects any of the proposed redactions, it will provide notice to the parties' counsel at least one week before releasing the decision publicly.

Signed by

Athanasios Hadjis
Tribunal Member

Ottawa, Ontario
August 11, 2025

Canadian Human Rights Tribunal

Parties of Record

Tribunal File: HR-DP-2972-23

Style of Cause: CB v. Canadian Security Intelligence Service

Ruling of the Tribunal Dated: August 11, 2025

Motion dealt with during a videoconference CMCC held July 9, 2025.

Oral representations by:

Samantha Lamb, for the Complainant

Korinda McLaine and Joshua Toews, for the Respondent