Federal Court  Cour fédérale

Date: 20181123

Docket: T-1616-17

Citation: 2018 FC 1179

Ottawa, Ontario, November 23, 2018

PRESENT: The Honourable Madam Justice Roussel

BETWEEN:

ALEX MARTINEZ

Applicant

and

COMMUNICATIONS SECURITY ESTABLISHMENT (CSE)

Respondent

JUDGMENT AND REASONS

I. Introduction

[1] The Applicant, Mr. Martinez, seeks judicial review of the response he received from the Respondent Communications Security Establishment [CSE] in answer to his request for access to his personal information. He brings this application pursuant to section 41 of the *Privacy Act*, RSC 1985, c P-21 [*Privacy Act*].

II. Background

[2] On January 26, 2017, Mr. Martinez wrote to the CSE requesting the following information:

> Please provide electronic copies of all files, including investigation files, officer's notes, records and audio and video surveillance records that are under my name and in the possession of the Communications Security Establishment. This includes documents created and sent to and from the Department of National Defence, The (sic) Royal Canadian Mounted Police, The (sic) Military Complaints Commission and the Canadian Security Intelligence Service (CSIS). All these organizations assisted and participated in internal investigations. There is no criminal record or abuse file for me in any organization or police force, nationally or internationally.

[3] In his letter to the CSE, Mr. Martinez states that he is a "former Consultant Sworn for the Government of British Columbia and the Government of Manitoba involved in an anti-corruption case and internal investigation with the [CSE]". He also states that the search "is part of a national and international search for those responsible for these offences and for opening false cases throughout Canada and abroad".

[4] Following receipt of the request, the CSE asked Mr. Martinez to give further direction on where to search for the requested information. In order to assist him, the CSE provided Mr. Martinez with an internet link containing a list of the Personal Information Banks [PIB] that applied to the CSE. On February 8, 2017, Mr. Martinez sent an email to the CSE consenting to the revised wording proposed by the CSE. The revised request reads as follows:

> Requesting all information in regards to Alex Martinez in Personal Information Banks PPU 040 (Foreign Intelligence Files), PPU 007 (Cyber Defence) and PSU 913 (Disclosure to Investigate Bodies).

[5] By letter dated March 10, 2017, the CSE responded as follows to the request of Mr. Martinez:

> Pursuant to section 16(2) of the Act, CSE neither confirms nor denies that records exist in the PPU 040: Foreign Intelligence Files. We are advising you, as required by paragraph 16(1)(b) of the [*Privacy Act*], that such records, if they existed, could reasonably be exempted under section 21 of the [*Privacy Act*]. No records could be located within PSU 913: Disclosure to Investigative Bodies and PPU 007: Cyber Defence.
>
> Please be advised that you are entitled to file a complaint with the Office of the Privacy Commissioner concerning the processing of your request.

[6] Mr. Martinez filed a complaint with the Office of the Privacy Commissioner of Canada [OPC] asserting that the CSE improperly denied him access to his personal information under the *Privacy Act*. He alleged that the CSE contravened the access provisions of the *Privacy Act* by failing to disclose any of the information he requested, by either refusing to confirm or deny the existence of information or by claiming that the information does not exist in its records.

[7] The OPC investigated the complaint of Mr. Martinez and concluded that it was not well-founded. In its Report of Findings dated September 13, 2017, the OPC explains that it examined the processing of the request in the course of its investigation and deemed the search conducted to locate the requested records to be appropriate. It then considered the validity of the exemptions claimed under sections 16, 18 and 21 of the *Privacy* Act and ultimately concluded that the CSE had acted in accordance with the *Privacy Act* in providing the response it did to Mr. Martinez.

[8] Not satisfied with this response, Mr. Martinez filed an application in this Court pursuant to section 41 of the *Privacy Act* on October 24, 2017. In the affidavit he submitted in support of his application, Mr. Martinez claims that the requested documents "are very important for correcting errors and uncovering crimes caused by criminal negligence and misconduct by officers in opposing police forces and organization". At the hearing, he claimed that he needed the requested information in order to bring various suspects to prosecution, following his investigation into what he alleges as the abuse of certain data systems by employees of the CSE and other organizations.

[9] On January 12, 2018, the CSE brought a motion pursuant to sections 46 and 51 of the *Privacy Act* for an order permitting it to file evidence and the records at issue on an *ex parte* basis and to make both written and oral *ex parte* representations to the Court. The motion was granted by the case management judge on March 7, 2018.

[10] Further to the order of the case management judge, the CSE filed a confidential affidavit with the Court on March 22, 2018 and a confidential record on June 21, 2018. After having had the opportunity to review and consider the confidential materials, on July 11, 2018, I presided over an *ex parte – in camera* hearing in Ottawa. Subsequent to the *ex parte – in camera* hearing, I issued a direction in which I indicated being satisfied that no additional information could be provided to Mr. Martinez and as a result, I directed that the matter be referred back to the judicial administrator so that a date could be set for the hearing during which Mr. Martinez could be present.

[11] On November 19, 2018, I presided over the hearing, which was conducted by means of a teleconference at the request of Mr. Martinez. Mr. Martinez, who is self-represented, had the opportunity to present his submissions to the Court and to reply to those made by counsel for the CSE. I also attempted to elicit some clarification on some of the allegations made by Mr. Martinez during the hearing.

III. Issues

[12] Upon review of the record before the Court and considering the submissions of both parties, I find that the determinative issues in this application are:

i. Did the CSE err by informing Mr. Martinez that there was no personal information relating to him in PIB PSU 913 and PPU 007?

ii. Did the CSE reasonably rely on subsection 16(2) of the *Privacy Act* when neither confirming nor denying the existence of personal information relating to Mr. Martinez in PIB PPU 040?

IV. Analysis

A. *Standard of review and burden of proof*

[13] When reviewing a government institution's decision not to disclose personal information, the Court undertakes a two (2) step process. The first step consists of determining, on a correctness standard of review, whether the withheld information actually falls within the statutory exemption. If the Court determines that the government institution properly relied upon

the claimed exemption, it must then proceed to determine whether the government institution, in cases where it is statutorily obligated to do so, appropriately exercised its discretion not to disclose said information. This review is conducted against a standard of reasonableness. As the decision not to release information that falls within the claimed exemption is heavily fact-based with a policy component, the reviewing Court is required to be deferential to the government institution's exercise of discretion (*Leahy v Canada (Citizenship and Immigration)*, 2012 FCA 227 at paras 96-100; *VB v Canada (Attorney General)*, 2018 FC 394 at para 30 [*VB*]; *Llewellyn v Canadian Security Intelligence Service*, 2014 FC 432 at para 23 [*Llewellyn*]; *Braunschweig v Canada (Public Safety)*, 2014 FC 218 at para 29 [*Braunschweig*]).

[14] Furthermore, the decision to adopt a blanket policy of neither confirming nor denying the existence of a record under subsection 16(2) of the *Privacy Act* is equally reviewable against the reasonableness standard as it involves the exercise of discretion (*Ruby v Canada (Solicitor General)*, [2000] 3 FC 589 (FCA), at paras 66-67 [*Ruby*], reversed on other grounds 2002 SCC 75; *VB* at para 31; *Westerhaug v Canadian Security Intelligence Service*, 2009 FC 321 at para 17 [*Westerhaug*]; *Cemerlic v Canada (Solicitor General)*, 2003 FCT 133 (FC) at para 44 [*Cemerlic*]).

[15] With respect to the burden of proof, section 47 of the *Privacy Act* clearly stipulates that it rests with the government institution (*Braunschweig* at para 30; *Cemerlic* at para 12).

B. *Did the CSE err by informing Mr. Martinez that there was no personal information relating to him in PIB PSU 913 and PPU 007?*

[16] PIB PPU 007 is a personal information bank established by the Minister of National Defence. It applies to personal information obtained as part of the CSE's statutory mandate set out in paragraph 273.64(1)(*b*) of the *National Defence Act*, RSC 1985, c N-5, which is to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada. Pursuant to subsection 273.64(2), the activities that are carried out under this part of the CSE's mandate shall not be directed at Canadians or any person in Canada and shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

[17] The current edition of "*InfoSource: Source of Federal Government and Employee Information*" [InfoSource], published by the CSE in accordance with section 11 of the *Privacy Act*, describes the nature of the information that is likely to be found in PIB PPU 007:

> **Communications Security Establishment (CSE) – Cyber Defence, CSE PPU 007 – Personal Information Bank**
>
> This bank relates to the personal information that may be collected by CSE during its assessment activities, in support of information infrastructures of importance to the Government of Canada to help them identify, isolate or prevent harm to their computer systems or networks. Personal information collected may include, full name, email address, IP address and any incidental personal information that is contained in electronic routing and identification information.

[18] As for PIB PSU 913, this personal information bank was created by the Treasury Board of Canada Secretariat [TBCS]. According to the current edition of "*Information about programs and information holdings*", also published by the TBCS in accordance with section 11 of the *Privacy Act*, the nature of the information likely to be found in PIB PSU 913 is described as follows:

> **Disclosure to Investigative Bodies**
>
> This bank describes personal information about individuals that may be requested by and/or disclosed to an investigative body pursuant to paragraph 8(2)(e) of the Privacy Act. The personal information may include any personal information element that a government institution collects about an individual as part of one of its authorized program or activity and that is subsequently requested by an investigative body listed in Schedule 2 of the Privacy Regulations.

[19] In his affidavit affirmed on March 16, 2018, the Director Disclosure, Policy and Review at the Operational and Corporate Policy Branch of the CSE [Director] states that thorough and appropriate searches were undertaken in PIB PSU 913 and PPU 007 and that no personal information concerning Mr. Martinez was located.

[20] Moreover, the search conducted by the CSE to locate the requested records was also found to be appropriate by the OPC.

[21] Based on the evidence before me, I am satisfied that the CSE did not err in its response to Mr. Martinez that no personal information relating to him was found in PIB PSU 913 and PPU 007.

C. *Did the CSE reasonably rely on subsection 16(2) of the Privacy Act when neither confirming nor denying the existence of personal information relating to Mr. Martinez in PIB PPU 040?*

[22] Section 18 of the *Privacy Act* allows the Governor in Council to designate as exempt banks certain personal information banks that contain files which consist predominantly of personal information described in sections 21 or 22 of the *Privacy Act* (*Braunschweig* at para

43). Under subsection 18(2) of the *Privacy Act*, the head of a government institution may refuse to disclose any personal information that is contained in a personal information bank that has been designated as exempt.

[23] In the case at hand, the Governor in Council designated PIB PPU 040 as an exempt bank based on section 21 of the *Privacy Act* (see *Order Respecting the Designation of the Security and Intelligence Information Files, No. ND-P70 as an Exempt Personal Information Bank*, cited as the *Exempt Personal Information Bank Order, No. 5 (ND)*, as published in the Canada Gazette, Part II, Vol. 119, No. 1 (SOR 85-38)).

[24] Section 21 of the *Privacy Act* provides that the head of a government institution may refuse to disclose personal information, "the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defense of Canada or any state allied or associated with Canada […] or the efforts of Canada toward detecting, preventing or suppressing subversive or hostile activities […]".

[25] The current edition of InfoSource describes PIB PPU 040 as follows:

> **Foreign Intelligence Files CSE PPU 040 - Personal Information Bank**
>
> **Description**: This bank contains personal information relating to sensitive aspects of Canada's international relations, security and defence.
>
> **Note**: This bank is designated by the Governor-in Council as an exempt bank pursuant to section 18(1) and based on section 21 of the *Privacy Act*. This PIB was transferred from the Department of National Defence.
>
> **Class of Individuals**: This bank applies to the general public.

> **Purpose**: The purpose of this bank is to advise the government regarding international affairs, security and defence.
>
> **Consistent Uses**: There are no other consistent uses.
>
> **Retention and Disposal Standards**: Information in this bank is held indefinitely.
>
> **RDA Number**: 98/005
>
> **Related Record Number**: CSE MIS 080
>
> **TBS Registration**: 20130231
>
> **Bank Number**: CSE PPU 040

[26] In his affidavit affirmed on March 16, 2018, the Director elaborates on the content and purpose of the information contained in PIB PPU 040:

> 27. As can be seen from its description (*InfoSource*), the exempt bank CSE PPU 040 contains predominantly sensitive national security information of the type described in section 21 of the *Privacy Act* that means personal information relating to sensitive aspects of Canada's international relations, security and defence.
>
> 28. The information in bank CSE PPU 040 is intended to support CSE's foreign intelligence collection operations, including target information of CSE operations and intelligence in regards to foreign individuals, states, organizations or terrorist groups, which has implications for Canada's international affairs, defence or security. …

[27] Like the OPC, I am satisfied that the PIB PPU 040 is an exempt personal information bank under section 18 of the *Privacy Act* and that, if any personal information relating to Mr. Martinez existed in the PIB PPU 040, it could reasonably be exempted under section 21 of the *Privacy Act*.

[28] In its response to Mr. Martinez, the CSE relied on subsection 16(2) to neither confirm nor deny the existence of the records contained in PIB PPU 040.

[29] The issue of whether a government institution can adopt a policy in view of neither confirming nor denying the existence of information is well established in the jurisprudence (*Braunschweig* at para 45). While the implementation of such a policy involves an exercise of discretion, it must be exercised reasonably in the context of the factual circumstances involved (*Cemerlic* at para 44).

[30] In *Ruby*, the Federal Court of Appeal held that the adoption of a policy of neither confirming nor denying the existence of information in a personal information bank was reasonable given the nature of the information bank in question. Merely revealing whether or not the institution has information on an individual would disclose to the concerned individual whether or not he or she was the subject of an investigation (*Ruby* at para 65). The Court explained further at para 66:

> … Elsewhere in the Act, the government has been given a wide scope for protecting secrecy of law enforcement related banks where secrecy is deemed appropriate. By providing the option under subsection 16(2) of refusing to confirm or deny the existence of personal information, Parliament offered one more such mechanism, allowing government institutions the possibility of maintaining not just the content but also the existence of records confidential. In the cat-and-mouse games that spies and criminals play with law enforcement agencies, for the agency to feel bound to reveal information in certain circumstances could create opportunities for educated guesses as to the contents of information banks based on a pattern of responses. To adopt a generalized policy of always refusing to confirm the existence of personal information eliminates this threat.

[31] The right of a government institution to neither confirm nor deny the existence of personal information, under subsection 16(2) of the *Privacy Act*, has been upheld by this Court (see *Braunschweig* at paras 45, 48; *Llewellyn* at paras 35-36; *Westerhaug* at paras 17-18; *Fuda v Canada (Royal Canadian Mounted Police)*, 2003 FCT 234 at paras 30-32; *Cemerlic* at paras 44-45).

[32] In the case at hand, the Director elaborates in his affidavit on the nature of the injury that would result if the CSE were to acknowledge the existence of information in the PIB PPU 040:

> 28. … Acknowledging the existence of information would inform a person as to whether their activities, as well as those of associates, have been subject of CSE foreign intelligence operations. Such knowledge allows for targets to take countermeasures, thereby compromising CSE's ability to carry out their mandate.
>
> 29. CSE's operations and ability to collect foreign intelligence, as per its mandate, could be negatively impacted by revealing whether or not it is in possession of the requested information. It could reasonably be expected that such disclosure would compromise CSE's ability to collect information to provide important foreign intelligence to the Government of Canada in line with its intelligence priorities, thereby causing injury to Canada's international relations, national defence and security.
>
> 30. There is a potential for wider injury than might be perceived by considering a piece or pieces of information without awareness of how that could be fitted with other information to provide a mosaic of significance to those seeking intelligence related to CSE's operations. While the mere revealing of the existence or non-existence of information in this case alone might be insignificant, if such disclosures were done on a regular basis, it would threaten the integrity of CSE's operations and hamper its ability to carry out its mandate.
>
> 31. Therefore, the response to the request for personal information must be the same whether or not such

> information exists: CSE will neither confirm nor deny the existence of information held in CSE PPU 040.

[33] Based on the evidence before me, I am satisfied that the CSE's discretion to adopt a policy to neither confirm nor deny the existence of personal information in PIB PPU 040 was reasonably exercised.

[34] Accordingly, the application for judicial review shall be dismissed. Given the result of the application, it is not necessary for me to address the other relief sought by Mr. Martinez, namely that of an "Order and Injunction to stop all investigations, suppression, observation and monitoring across Canada and internationally" and "Costs and damages" in the amount of $9,000,000.00.

[35] As for costs, the CSE is seeking costs and disbursements in the amount of $6,051.00. Mr. Martinez disagrees that these costs should be payable for the following alleged reasons: i) the costs were incurred improperly by way of misconduct or without reasonable cause; ii) the CSE has unlimited resources to cover the expenses of the solicitor and thus, a cost award would constitute an abuse of power as he has been without an income since 2012; and iii) considering the CSE's budget, power and range as well as the fact that he "assisted and exposed corruption and scandal within the organization, which subsequently saved several employees and senior staff", the Bill of Costs is "clearly 'comparative negligence,' an 'abuse of process,' and 'frivolous and vexatious.'"

[36] Subsection 52(1) of the *Privacy Act* provides that cost awards are in the discretion of the Court and shall follow the event unless the Court orders otherwise. Given the particular circumstances of this case, I have decided, in the exercise of my discretion, that no costs shall be awarded.

JUDGMENT in T-1616-17

THIS COURT'S JUDGMENT is that:

1. The application for judicial review is dismissed.

2. No costs are awarded.

"Sylvie E. Roussel"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-1616-17
STYLE OF CAUSE:	ALEX MARTINEZ v COMMUNICATIONS SECURITY ESTABLISHMENT (CSE)
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	NOVEMBER 19, 2018 (BY TELECONFERENCE)
JUDGMENT AND REASONS:	ROUSSEL J.
DATED:	NOVEMBER 23, 2018

APPEARANCES:

Alex Martinez	FOR THE APPLICANT (SELF-REPRESENTED)
Marieke Bouchard	FOR THE RESPONDENT

SOLICITORS OF RECORD:

Attorney General of Canada Ottawa, Ontario	FOR THE RESPONDENT