Federal Court  Cour fédérale

Date: 20220725

Docket: T-1814-19

Citation: 2022 FC 1100

Ottawa, Ontario, July 25, 2022

PRESENT: The Honourable Madam Justice Kane

BETWEEN:

NAVARATNAM KANDASAMY

Applicant

and

THE MINISTER OF PUBLIC SAFETY

Respondent

JUDGMENT AND REASONS

[1] The Applicant, Mr. Navaratnam Kandasamy, brings this Application for Judicial Review pursuant to section 41 of the *Privacy Act*, RSC 1985, c P-21 [the Act] of the decision of the Minister of Public Safety [Public Safety], dated February 25, 2019 in response to Mr. Kandasamy's request for personal information.

[2] Mr. Kandasamy argues that the Minister of Public Safety erred in not disclosing personal information, which Mr. Kandasamy claims is held in data banks maintained by Public Safety. He seeks an order from this Court that the information be disclosed to him.

[3] Mr. Kandasamy has not raised any specific errors in the decision, but rather asserts his belief that information about him has been collected and retained and should be disclosed.

[4] Mr. Kandasamy asserts that he has been tracked, followed and criminally harassed within Canada and in foreign countries and that his communications have been hacked and/or deleted. He contends that he has been and continues to be under constant surveillance by several unnamed agencies. He alleges that he has been "penetrated by energy weapons" and targeted in other ways, all of which impacts his daily life. He also believes that incorrect information about him has been shared with other countries, and he alleges that he was mistreated when he travelled abroad between 2008 and 2010. He attests that he made complaints to the local police, who did not respond.

[5] Mr. Kandasamy also seeks judicial review of two other decisions regarding requests for his personal information. In file T-167-20, he challenges the decision of the Canadian Security Intelligence Service [CSIS] and in file T-953-20, he challenges the decision of the Royal Canadian Mounted Police [RCMP]. The three applications were heard together. Mr. Kandasamy sought similar information from CSIS and RCMP and made similar claims about the nature of the information he believes is retained by those agencies. He also made similar arguments in the

three applications and reiterated his concerns that he is being monitored, surveilled and generally mistreated.

[6] Mr. Kandasamy would have benefitted from independent legal advice and representation. He explained that he was not able to retain counsel due to the cost and/or because legal aid was not available and/or because counsel he consulted claimed to be unfamiliar with the Act or the legal issues he sought to raise. However, counsel may have been better able to explain to Mr. Kandasamy the principles underlying the Act and how it operates to both provide information and protect other information from disclosure. Counsel could, perhaps, also have directed Mr. Kandasamy to resources to address his fears and beliefs, which were not supported by any evidence before this Court. In addition, counsel may have been better able to explain that a judicial review focusses on whether the government institution—in this case the Minister of Public Safety—reasonably applied the exemptions in the Act.

[7] Despite the challenges faced by Mr. Kandasamy in making his submissions, in accordance with section 47 of the Act, the burden is on the government institution to establish that it is authorized to refuse to disclose the information sought. I am satisfied that Public Safety has established that its response to Mr. Kandasamy was both reasonable and mandated by the Act.

I. **Background**

A. *The Request*

[8] On January 3, 2019, Mr. Kandasamy submitted a Personal Information Request Form to the Department of Public Safety and Emergency Preparedness (as it was then known) seeking the disclosure of all records under the control of Public Safety dated from April 4, 1991 to January 7, 2019, containing Mr. Kandasamy's personal information.

[9] Due to the lack of clarity in Mr. Kandasamy's Personal Information Request Form, Public Safety redrafted the request with the consent of Mr. Kandasamy as follows:

> Any and all records under the control of Public Safety Canada that contain personal information belonging to Navaratnam Kandasamy … as defined under section 3 of the *Privacy Act* (the *Act*), dated from April 4, 1991 – January 7, 2019, including (but not limited to) the following banks/documents:
>
> 1. National Security (bank #: PSPPU026)
> 2. Records shared internationally (be they with partners and/or countries) by the International Affairs Division (including, but not limited to, Sri Lanka, India and the United Kingdom) (record #: PSPACB-02)
> 3. National Crime Prevention strategy flagging system (including, but not limited to, information sharing on victim issues/inquiries, corresponding records, contracts, or any other new and existing government programming) (bank #: PSPPU039)
> 4. Background checks (i.e., related to security clearance)
> 5. Invasion of privacy (record #: PsNcSb-09)

6. Any personal communication related to permanent and continued domestic electronic surveillance (record #: PSNCSB09)

[10] The Access to Information Analyst distributed the request to the relevant branches within Public Safety in order to identify any records that responded to the request. The Portfolio Affairs and Communications Branch identified 78 pages of records, consisting of communications received by Public Safety from Mr. Kandasamy relating to his concerns about being under surveillance.

B. *Public Safety's Response*

[11] Mr. Kandasamy's request for information in the National Security Bank included a search by Public Safety of the Passenger Protect Program data bank.

[12] Access to Information and Privacy Manager, Mr. André Chartrand, could not confirm or deny that any such information existed in the Passenger Protect Program data bank due to the impact that such information could have on Canada's ability to combat aviation security threats. Mr. Chartrand also noted that subsection 20(2) of the *Secure Air Travel Act*, SC 2015, c 20, s 11, prohibited disclosure of information about whether a person is listed in the Passenger Protect Program.

[13] On February 25, 2019, Mr. Chartrand advised Mr. Kandasamy by letter that his request had been processed. As noted, information, which consisted of personal communications

between Mr. Kandasamy and various public officials relating to his concerns about surveillance, was disclosed. The letter further stated:

> Pursuant to subsection 16 of the [*Privacy*] *Act*, we neither confirm nor deny that some of the records that you requested exist. We are, however, advising you, as required by paragraph 16(1)(b) of the *Act*, that such records, if they existed, could reasonably be expected to be exempted under section 21 (as it relates to the efforts of Canada towards detecting, preventing or suppressing subversive or hostile activities).

[14] Dissatisfied with this response, Mr. Kandasamy made a complaint to the Privacy Commissioner.

C. *The Report of the Office of the Privacy Commissioner*

[15] By letter dated September 12, 2019, a Senior Privacy Investigator [the Investigator] advised Mr. Kandasamy that the Office of the Privacy Commissioner [OPC] had opened a file to investigate his complaint. The Investigator noted, based on a preliminary review, that Mr. Kandasamy's request included a search of the National Security Bank, which holds information pertaining to the Passenger Protect Program. The Investigator advised Mr. Kandasamy that all government departments are bound by law to neither confirm nor deny the existence of information pertaining to an individual that relates to the Passenger Protect Program.

[16] By letter dated September 19, 2019, the Investigator advised Mr. Kandasamy that following the investigation of his complaint, the OPC had concluded that the complaint was not well founded. The report of the Investigator describes Mr. Kandasamy's request for information, the relevant provisions of the Act, in particular sections 16 and 21, and confirms that if the

requested information existed, it would be exempt pursuant to section 21. The OPC concluded that Public Safety complied with the Act in responding to the request for information.

II. **Relevant Statutory Provisions**

Privacy Act	*Loi sur la protection des renseignements personnels*
2 The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.	**2** La présente loi a pour objet de compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès des individus aux renseignements personnels qui les concernent.
4 No personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution.	**4** Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités.
16 (1) Where the head of a government institution refuses to give access to any personal information requested under subsection 12(1), the head of the institution shall state in the notice given under paragraph 14(a)	**16 (1)** En cas de refus de communication de renseignements personnels demandés en vertu du paragraphe 12(1), l'avis prévu à l'alinéa 14a) doit mentionner, d'une part, le droit de la personne qui a fait la demande de déposer une plainte auprès du Commissaire à la protection de la vie privée et, d'autre part :
(a) that the personal information does not exist, or	**a)** soit le fait que le dossier n'existe pas;
(b) the specific provision of this Act on which the	**b)** soit la disposition précise de la présente loi

refusal was based or the provision on which a refusal could reasonably be expected to be based if the information existed,	sur laquelle se fonde le refus ou sur laquelle il pourrait vraisemblablement se fonder si les renseignements existaient.
and shall state in the notice that the individual who made the request has a right to make a complaint to the Privacy Commissioner about the refusal.	
(2) The head of a government institution may but is not required to indicate under subsection (1) whether personal information exists.	(2) Le paragraphe (1) n'oblige pas le responsable de l'institution fédérale à faire état de l'existence des renseignements personnels demandés.
21 The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada, as defined in subsection 15(2) of the *Access to Information Act*, or the efforts of Canada toward detecting, preventing or suppressing subversive or hostile activities, as defined in subsection 15(2) of the *Access to Information Act*, including, without restricting the generality of the foregoing, any such information listed in paragraphs 15(1)(a) to (i) of the *Access to Information Act*.	**21** Le responsable d'une institution fédérale peut refuser la communication des renseignements personnels demandés en vertu du paragraphe 12(1) dont la divulgation risquerait vraisemblablement de porter préjudice à la conduite des affaires internationales, à la défense du Canada ou d'États alliés ou associés avec le Canada, au sens du paragraphe 15(2) de la *Loi sur l'accès à l'information*, ou à ses efforts de détection, de prévention ou de répression d'activités hostiles ou subversives, au sens du paragraphe 15(2) de la même loi, notamment les renseignements visés à ses alinéas 15(1)a) à i).

41 Any individual who has been refused access to personal information requested under subsection 12(1) may, if a complaint has been made to the Privacy Commissioner in respect of the refusal, apply to the Court for a review of the matter within forty-five days after the time the results of an investigation of the complaint by the Privacy Commissioner are reported to the complainant under subsection 35(2) or within such further time as the Court may, either before or after the expiration of those forty-five days, fix or allow.

41 L'individu qui s'est vu refuser communication de renseignements personnels demandés en vertu du paragraphe 12(1) et qui a déposé ou fait déposer une plainte à ce sujet devant le Commissaire à la protection de la vie privée peut, dans un délai de quarante-cinq jours suivant le compte rendu du Commissaire prévu au paragraphe 35(2), exercer un recours en révision de la décision de refus devant la Cour. La Cour peut, avant ou après l'expiration du délai, le proroger ou en autoriser la prorogation.

47 In any proceedings before the Court arising from an application under section 41, 42 or 43, the burden of establishing that the head of a government institution is authorized to refuse to disclose personal information requested under subsection 12(1) or that a file should be included in a personal information bank designated as an exempt bank under section 18 shall be on the government institution concerned.

47 Dans les procédures découlant des recours prévus aux articles 41, 42 ou 43, la charge d'établir le bien-fondé du refus de communication de renseignements personnels ou le bien-fondé du versement de certains dossiers dans un fichier inconsultable classé comme tel en vertu de l'article 18 incombe à l'institution fédérale concernée.

[Emphasis added.]

[Je souligne.]

Secure Air Travel Act

Loi sur la sûreté des déplacements aériens

20 (1) It is prohibited to disclose the list, except as required for the purposes of sections 10, 11, 12 and 13.

20 (1) Il est interdit de communiquer la liste, sauf pour l'application des articles 10, 11, 12 et 13.

(2) It is prohibited to disclose whether or not any individual is or was a listed person, except	**(2)** Il est interdit de communiquer le fait qu'une personne est, a été, n'est pas ou n'a pas été une personne inscrite, sauf :
(a) for the purposes of sections 10 and 10.3 to 16;	**a)** pour l'application des articles 10 et 10.3 à 16;
(b) as required to enforce any law of Canada or a province or to carry out a lawful activity;	**b)** si cela est nécessaire pour le respect des lois fédérales ou provinciales ou pour la tenue d'activités licites;
(c) for the purpose of complying with a subpoena or document issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;	**c)** en conformité avec un subpoena, un document ou une ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou avec des règles de procédure se rapportant à la production de renseignements;
(d) in the case where an individual discloses that he or she is or was a listed person; or	**d)** si une personne communique le fait qu'elle-même est ou a été une personne inscrite;
(e) if the Minister has disclosed under section 12.1 that the individual is not a listed person, in the case where anyone further discloses that information.	**e)** si le ministre a communiqué au titre de l'article 12.1 le fait que cette personne n'est pas une personne inscrite, dans le cas où ce renseignement est communiqué à nouveau par quiconque.

III. **The Issues and Standard of Review**

[17] Section 41 of the Act provides for review of the decision to this Court, but does not specify the standard of review. Section 41 of the Act differs from the parallel provision in section

44.1 of the *Access to Information Act*, RSC 1985, c A-1 [ATIA], which provides that a review is to be conducted as a *de novo* proceeding.

[18] The law is well established that judicial review pursuant to section 41 of the Act is a two-step process; first, the Court determines whether the requested information is subject to the exemptions relied on, and second, the Court determines whether the government institution reasonably exercised its discretion to withhold the disclosure of the information. The decision of the Supreme Court of Canada in *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 [*Vavilov*], which establishes that reasonableness is the presumptive standard of review, has resulted in both steps of the two-step process being reviewed on the reasonableness standard. As explained by this Court in *Chin v Canada (Attorney General*), 2022 FC 464 at paras 14–17 [*Chin*]:

> [14] Judicial review of a government institution's refusal to disclose information involves a two-step process (*Russell v Canada (Attorney General)*, 2019 FC 1137 [*Russell*] at para 24). The first step requires the Court to consider if the requested information, whether actual or hypothetical, falls within the legislative provisions relied upon. The second step requires the Court to consider the government's exercise of its discretion not to disclose the requested information.
>
> [15] Prior to the Supreme Court of Canada's decision in *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 [Vavilov], the first step was understood to be reviewable against the standard of correctness, while the second step was reviewable against the standard of reasonableness (*Braunschweig v Canada (Public Safety*), 2014 FC 218 [*Braunschweig*] at para 29; *Llewellyn v Canadian Security Intelligence Service*, 2014 FC 432 [*Llewellyn*] at para 23).
>
> [16] However, in *Vavilov* the Supreme Court of Canada held that the standard of review must reflect the legislature's intent with respect to the role of the reviewing court, except where giving effect to that intent is precluded by the rule of law. The starting

> point for the analysis is a presumption that the legislature intended the standard of review to be reasonableness (*Vavilov* at para 23).
>
> [17] There is nothing to rebut the presumption of reasonableness review for both steps of the analysis, and accordingly the Court will intervene only if "there are sufficiently serious shortcomings in the decision such that it cannot be said to exhibit the requisite degree of justification, intelligibility and transparency" (*Vavilov* at para 100). A decision not to release information that falls within a claimed exemption is heavily fact-based with a policy component, and the Court therefore owes deference to a government institution's exercise of discretion (*Martinez v Canada (Communications Security Establishment)*, 2018 FC 1179 at para 13).

[19] In *Martinez v Canada (Communications Security Establishment)*, 2018 FC 17 [*Martinez*], the Court confirmed, at para 14, that decisions to neither confirm nor deny the existence of a record are also reviewed on the reasonableness standard. This continues to reflect the law.

[20] The issue is, therefore, whether Public Safety reasonably applied the statutory provisions and exemptions and reasonably exercised its discretion not to disclose the information sought.

IV. **The Applicant's Submissions**

[21] Mr. Kandasamy asserts that Public Safety erred by relying on section 21 of the Act to decline to disclose the personal information he sought. He also asserts that Public Safety erred by refusing to confirm or deny the existence of other information. Mr. Kandasamy did not identify any particular errors in the decision.

[22] Mr. Kandasamy's submissions relate to his ongoing belief that he has been a victim of cyber torture, was mistreated (without providing any details) and remains under surveillance. As

a result, he believes that records about him exist and should be provided to him to ensure accountability of public officials.

[23] As in his written submissions in the related applications, Mr. Kandasamy referred to excerpts from news articles, websites and other thoughts and opinions about surveillance techniques, mind control, artificial intelligence, and microwave weapons, none of which have any relevance to the issues before the Court.

V. **The Respondent's Submissions**

[24] The Respondent notes that Canadian citizens and permanent residents have a right to request and be given access to personal information that is contained within a personal information data bank or is otherwise under the control of a government institution if they are able to provide sufficient detail to permit retrieval of that information. The Respondent points to *Info Source: Sources of Federal Government and Employee Information* for the descriptions of the content of various data banks, including the National Security data bank and the Passenger Protect Program data bank. The Respondent further notes that the Act, while permitting access to information, has reasonable limits and exemptions.

[25] The Respondent submits that Public Safety reasonably determined that the information requested by Mr. Kandasamy, if it existed, would be exempt from disclosure pursuant to section 21 of the Act. In addition, the Respondent submits that it was reasonable for Public Safety to refuse to confirm or deny the existence of the requested information pursuant to subsection 16(2) of the Act.

[26] The Respondent notes that section 21 of the *Privacy Act* is an injury-based exemption, which requires the decision maker to determine whether the release of the information could prejudice the interests set out in the exemption. The Respondent points to *Braunschweig v Canada (Public Safety)*, 2014 FC 218 at paras 33–34, where the Court noted the types of exemptions:

> [34] Both the Act and the ATIA provide two types of exemptions from disclosure: class-based exemptions and injury-based exemptions. This Court has summarized the distinction between the two classes in *Bronskill v Canada (Minister of Canadian Heritage)*, 2011 FC 983 at para 13, [2011] FCJ No 1199:
>
> > [13] The exemptions laid out in the Act are to be considered in two aspects by the reviewing Court. Firstly, exemptions in the Act are either class-based or injury-based. Class-based exemptions are typically involved when the nature of the documentation sought is sensitive in and of itself. For example, the section 13 exemption is related to information obtained from foreign governments, which, by its nature, is a class-based exemption. Injury-based exemptions require that the decision-maker analyze whether the release of information could be prejudicial to the interests articulated in the exemption. Section 15 is an injury-based exemption: the head of the government institution must assess whether the disclosure of information could "be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities".
>
> [34] In addition, the exemptions under the Act and the ATIA can be categorized as either mandatory or discretionary, depending on the wording of the provision creating the exemption –whether the government "shall refuse to disclose" or "may refuse to disclose". This means that depending on the provision relied upon, the government can be obligated to enforce the exemption or it can have the discretion to decide whether or not to enforce it.

[27] The Respondent explains that the interests set out in section 21 are very broad. The decision maker must determine whether the disclosure of information could be expected to be injurious to the conduct of international affairs, the defence of Canada or the detection, prevention or suppression of subversive or hostile activities. The role of the Court on judicial review is to assess the reasonableness of this determination.

[28] The Respondent submits that Public Safety's response was reasonable because Mr. Kandasamy sought access to the National Security Bank, which includes information on persons whose activities are suspected of constituting threats to the security of Canada, and information about the Passenger Protect Program, which identifies persons who may pose a threat to aviation security. The Respondent notes that these records are created for the purpose of detecting and preventing activities as described in subsection 15(2) of the ATIA. Disclosure of such information would be injurious to the detection of such activities. Releasing information that would confirm an investigation of this type would cause an injury, which engages section 21 of the Act.

[29] The Respondent further submits that it was reasonable for Public Safety to refuse to confirm or deny the existence of the requested information pursuant to subsection 16(2) of the Act. Moreover, Public Safety was legally required to withhold disclosure in accordance with subsection 20(2) of the *Secure Air Travel Act*, which prohibits disclosure of whether or not any person is or was listed in the Passenger Protect Program.

[30] The Respondent explains that confirming whether or not the information exists would be contrary to the objectives of the Passenger Protect Program as it would alert persons who potentially pose a risk as to whether they are under scrutiny. The Respondent notes that any person who seeks such information will receive the same response.

VI. **The Decision Is Reasonable**

[31] The Act begins with a statement of its purpose in section 2, which is to protect the privacy of individuals with respect to personal information about themselves held by a government institution and to provide individuals with a right to access that information. However, the right of access that an individual has to personal information held in various data banks is subject to limitations.

[32] Mr. Kandasamy appears to believe that Public Safety and other agencies collect a vast amount of information about him, and are mandated to do so. However, section 4 of the Act provides that a government institution's collection of personal information must relate to an operating program or activity of that government institution. As noted by the Respondent, *Info Source* describes the various data banks held by government institutions. Mr. Kandasamy has not explained the basis for his belief that information about him even exists in any data bank.

[33] Mr. Kandasamy has also not addressed the relevant issue on this Application, which is whether the response by Public Safety to his request for personal information is reasonable. Regardless of the lack of any coherent submissions, the Court has considered the relevant issues, the statutory provisions and the jurisprudence.

[34] In accordance with section 47 of the Act, the burden is on the government institution—in this case, Public Safety—to justify that it was reasonable to conclude that the requested information, if it existed, would be exempt from disclosure pursuant to section 21, and that it was reasonable to refuse to confirm or deny the existence of that information pursuant to subsection 16(2).

[35] Mr. Kandasamy's request for information included information contained in the National Security data bank, which also includes information in the Passenger Protect Program data bank. These records, if they exist, are maintained in order to detect and prevent hostile activities as described in subsection 15(2) of the ATIA, which is referred to in section 21 of the Act.

[36] Mr. André Chartrand explained in his affidavit that if Public Safety disclosed whether or not it had certain records, this information could be used to learn whether a person was included in the Passenger Protect Program, the nature of the investigation into the perceived security threat or other security information. This could jeopardize efforts to prevent security threats.

[37] I agree with the Respondent that disclosure of such records—if indeed they existed—would be injurious to the detection or prevention of such activities. Confirming whether this information exists would not be in the national interest, as it would alert a person who may pose a security risk that they are included in the Passenger Protect Program and are under scrutiny.

[38] The jurisprudence has established that releasing information that confirms investigations related to the interests set out in section 21 would cause an injury and that such information falls

within the exemptions set out in subsection 15(1) of the ATIAand section 21 of the Act: see for example *VB v Canada (Attorney General)*, 2018 FC 394 [*VB*]; *Westerhaug v Canadian Security Intelligence Service*, 2009 FC 321 [*Westerhaug*]; *Russell v Canada (Attorney General)*, 2019 FC 1137 [*Russell*]; *Chin* (all in the CSIS context, but the same principle applies here).

[39] I find that it was reasonable for Public Safety to determine that the requested information—if it existed—would be exempt from disclosure under section 21 of the Act.

[40] This conclusion does not signal that Mr. Kandasamy is regarded as a security risk. Rather, this is the explanation for why the hypothetical information he seeks cannot be provided to him.

[41] I also find that it was reasonable for Public Safety to refuse to confirm or deny the existence of the information requested by Mr. Kandasamy pursuant to subsection 16(2) of the Act.

[42] Subsection 16(2) provides that the head of the government institution (to which the request for information is made) is not required to indicate whether or not the personal information exists.

[43] In addition, subsection 20(2) of the *Secure Air Travel Act* prohibits the disclosure of whether or not a person is or was listed in the Passenger Protect Program. Although there are

some exceptions, the exceptions generally apply to permit disclosure to those engaged in ensuring safe air travel and national security, and none apply to the present circumstances.

[44] Therefore it was both reasonable and legally required for Public Safety to refuse to confirm or deny that the information existed.

[45] In *Ruby v Canada (Solicitor General)*, [2000] 3 FC 589, 2000 CanLII 17145 (FCA) [*Ruby*], the Federal Court of Appeal found that the general or blanket policy of a government institution to neither confirm nor deny the existence of information in accordance with subsection 16(2) is reasonable, and explained at paras 65–67,

> [65] The factual context we are dealing with in the present instance is that of requests for personal information concerning lawful investigations. Given the nature of the bank in question, the mere revealing of the existence or non-existence of information is in itself an act of disclosure: a disclosure that the requesting party is or is not the subject of an investigation.
>
> [66] In these factual circumstances, the particular nature and purpose of the Act and subsection 16(2) indicate that it was a reasonable exercise of discretion to adopt a general policy of never confirming the existence of information in the bank in question. 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.

> [67] Given the particular context and legislative intent we are dealing with here, it seems appropriate that discretion not be exercised on a case-by-case basis in relation to the bank in question. While generally administrative decision makers should not fetter their discretion by adopting a general rule of always responding the same way to certain requests, this is one of those rare instances where the adoption of a general policy is itself a judicious exercise of discretion.
>
> [Emphasis added.]

[46] More recently, the Court considered the same issue in *VB* in the context of a decision of CSIS; however, the same principles apply to the present case. The Court noted:

> [41] The ATIA expressly recognizes that in responding to a request for records or documents under the control of a government institution, the head of the government institution may decline to indicate if a record exists (ATIA, subsection 10(2)). A parallel provision is found at subsection 16(2) of the *Privacy Act*.
>
> [42] In considering the *Privacy Act* provision the Federal Court of Appeal has concluded: (1) subsection 16(2) permits a government institution to adopt a policy of neither confirming nor denying the existence of information where the information is of a specified type or nature; (2) adopting such a policy involves the exercise of a discretion; and (3) the discretion must be exercised reasonably (*Ruby* at paras 66-67).
>
> [43] The CSIS practice of neither confirming nor denying the existence of records where the information sought relates to CSIS investigative records has been consistently held to be reasonable where the information has been sought pursuant to the *Privacy Act* (*Llewellyn* at para 37, *Cemerlic* at paras 44 and 45, *Westerhaug* at para 18). The jurisprudence has found that confirming whether such information exists or not would be contrary to the national interest as it would alert individuals who potentially present a security risk as to whether they are the target of a CSIS investigation.
>
> […]
>
> [47] The PIB reference in the CSIS response is not a confirmation that records of the nature sought are held by CSIS. Instead the CSIS response in neither confirming nor denying the

> existence of the records opens the door to two equally possible scenarios: (1) the records exist but are not being disclosed on the basis that they are exempt from disclosure pursuant to sections 15 and 16 of the ATIA; or (2) no records exist. The absence of certainty this circumstance creates may understandably cause frustration to a requester but this situation is not unique to the applicant. As was noted by Justice Russel Zinn in *Westerhaug:*
>
> > [18] The Federal Court of Appeal in *Ruby* held that adopting a policy of non-disclosure was reasonable given the nature of the information bank in question, because merely revealing whether or not the institution had information on an individual would disclose to him whether or not he was a subject of investigation. I agree. If it is in the national interest not to provide information to persons who are the subject of an investigation, then it follows that it is also in the national interest not to advise them that they are or are not the target of an investigation. It is one of the unfortunate consequences of adopting such a blanket policy that persons who are not the subject of an investigation and who have nothing to fear from the government institution will never know that they are not the subject of an investigation. Nonetheless, and as was noted by Justice Kelen, this policy applies to every citizen of the country, and even judges of this Court would receive the same response as was given to Mr. Westerhaug and would not have any right to anything further. [Emphasis added.]

[47] It is well established that government institutions may reasonably refuse to confirm or deny the existence of information that could reveal whether a person is or has been the subject of an investigation. (See for example *Ruby* at paras 65ff; *Braunschweig* at paras 45, 48; *Llewellyn v Canadian Security Intelligence Service*, 2014 FC 432 at paras 35–36; *Westerhaug* at paras 17-18; *Martinez* at paras 30–31; *Russell* at para 26; *Chin* at paras 21–22).

[48] As in *VB*, *Westerhaug* and many other cases, the response that Mr. Kandasamy received is the same response that any other person requesting the same information would receive. There is nothing unusual, exceptional or unreasonable in the response provided by Public Safety to Mr. Kandasamy.

[49] In conclusion, I appreciate that Mr. Kandasamy may sincerely believe that records exist about him that he should be able to access. However, as noted, he has not explained the reason for his belief. Moreover, there is no error in the decision of Public Safety with respect to Mr. Kandasamy's request for personal information. As explained at the hearing of this Application, the Court's role is to determine the reasonableness of the decision—it is not to respond to the many other allegations regarding mistreatment and cyber torture. In addition, as explained to Mr. Kandasamy at the hearing, in response to his request that the Court order a Commission of Inquiry into his alleged mistreatment, this is not the Court's role on judicial review and there is absolutely no evidence before this Court of any mistreatment by anyone toward Mr. Kandasamy.

VII. **Costs**

[50] The Respondent seeks nominal lump sum costs of $750 in total for this Application and the two related applications, T-167-20 and T-953-20 (or alternatively, $250 for each application). The Respondent acknowledges that the Applicant is self- represented, but notes that the Applicant caused delays in the determination of the three applications and that the applications were unnecessary.

[51] Rule 400 provides that the Court has discretion to determine whether costs should be awarded and in what amount. The non-exhaustive factors set out in Rule 400(3) provide guidance to the Court in making this determination (*Francosteel Canada Inc v African Cape (The),* 2003 FCA 119). The factors include the result of the proceeding; the importance and complexity of the issues; the amount of work; the conduct of a party that tended to shorten or lengthen the proceeding; whether any step in the proceeding was improper, vexatious or unnecessary; and any other matter that the Court considers relevant. The result of the proceeding usually carries significant weight because, as a general rule, costs should follow the event (*Merck & Co Inc v Novopharm Ltd*, 1998 CanLII 8260 at para 24, 152 FTR 74 (FCTD)).

[52] In the present case, the Respondent is entitled to the nominal costs requested given the time and effort incurred in responding to the three applications, including the preparation of affidavits, and given their success.

JUDGMENT in file T-1814-19

THIS COURT'S JUDGMENT is that:

1. The Application for Judicial Review is dismissed.
2. The Applicant shall pay the Respondent costs in the amount of $250 for this Application.

"Catherine M. Kane"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-1814-19
STYLE OF CAUSE:	NAVARATNAM KANDASAMY v MINISTER OF PUBLIC SAFETY
PLACE OF HEARING:	HELD BY VIDEOCONFERENCE
DATE OF HEARING:	JULY 5, 2022
REASONS FOR JUDGMENT AND JUDGMENT:	KANE J.
DATED:	JULY 25, 2022

APPEARANCES:

Navaratnam Kandasamy	ON HIS OWN BEHALF
Jacob Blackwell	FOR THE RESPONDENT

SOLICITORS OF RECORD:

None	FOR THE APPLICANT
Attorney General of Canada Toronto, Ontario	FOR THE RESPONDENT