Federal Court  Cour fédérale

Date: 20150922

Docket: T-551-15

Citation: 2015 FC 1101

Ottawa, Ontario, September 22, 2015

PRESENT: The Honourable Madam Justice Kane

BETWEEN:

THE PROFESSIONAL INSTITUTE OF THE PUBLIC SERVICE OF CANADA AND STÉPHANE AUBRY

Applicants

and

ATTORNEY GENERAL OF CANADA

Respondent

ORDER AND REASONS

Overview

[1] The applicants, the Professional Institute of the Public Service of Canada [PIPSC], the bargaining agent which represents 35,000 scientists and professionals employed by the Government of Canada, and Stéphane Aubry, an employee, member of PIPSC and its part-time Vice-President, seek an interlocutory injunction to prevent the Treasury Board of Canada, on

behalf of the Government of Canada, from implementing the 2014 *Standard on Security Screening* [2014 Standard or Standard] pending the final determination of the applicants' application for judicial review of the government's decision to implement the Standard.

[2] The applicants' motion for the interlocutory injunction targets particular aspects of the Standard, including but not limited to credit checks, criminal record checks (requiring fingerprinting), open source inquiries, and requirements to update the employer on changes in an employee's status and ongoing monitoring, referred to as "after-care".

[3] To succeed on the motion for an interlocutory injunction, the applicants must establish that a serious issue has been raised, that the applicants will suffer irreparable harm if the injunction is not granted and the implementation of the Standard continues, and that the balance of convenience, which assesses the harm to the applicants, the harm to respondent and includes an assessment of the public interest, favours the applicants.

[4] For the reasons elaborated on below, I find that the applicants have raised one or more serious issues that will be determined on judicial review, but have not provided any concrete evidence that irreparable harm will be suffered by any of the union's members between now and the time that the judicial review is finally disposed of.

[5] The jurisprudence has clearly established that all three elements of the test for an injunction must be established and that independent and concrete evidence, rather than general and speculative assertions of irreparable harm, must be provided. The applicants' assertion that

the requirement to provide information for a security clearance, by its very nature, amounts to a loss of privacy overlooks, among other things, the many safeguards in place to protect the information, including ensuring that it is not disclosed to anyone other than designated Security Officers within government departments, and overlooks that many of the measures at issue are not unprecedented and could have been required under the 1994 *Personnel Security Standard* [1994 Standard] and as updated in 2002.

[6] It should have been a simple matter to provide an affidavit from Mr Aubry or other members of the union indicating their position, existing security level and the date of its expiry to establish that some particular employee(s) would be subjected to the new measures in the period pending the judicial review and describing the harm that employee would suffer by submitting themself to the measures at issue. Had such evidence been provided, the respondent and the Court would have had an opportunity to test and assess the evidence to determine whether irreparable harm had been established. Rather, the applicants simply assert that it is a foregone conclusion or a matter of common sense for the Court to conclude that it is obvious that some or many of the 35,000 members of its union will be subjected to the new measures in the near future and will suffer harm.

[7] The applicants must do more than make assertions and ask the Court to make assumptions and rely on common sense, rather than on the law.

[8] With respect to the balance of convenience, the relative harm to the applicants and respondent has been assessed and the harm to the public good has been considered in this context.

[9] The respondent has established to the satisfaction of the Court that the 2014 Standard was developed and implemented in the public interest. The Court need not determine if that is so at this stage; it is presumed to be so. As a result, enjoining the implementation of the Standard is assumed to result in harm to the public good.

[10] The applicants have not offered any evidence to overcome this assumption and to show that the public interest would be harmed by continuing to implement the Standard pending the determination of the judicial review. Nor have they provided concrete evidence of other harm to them. Information required to be provided by applicants in accordance with the Standard pending the determination of the judicial review will be safeguarded and will not be disclosed, redress mechanisms exist, and an employee's ongoing employment will not be at risk to any greater extent than under the previous Standard. The applicants have not established that the harm to them, if the injunction is not granted, is greater than the harm to the respondents, if the injunction is granted.

[11] The government has launched the new Standard and is in the process of fully implementing it over a 36 month period. Although the implementation is at an early stage, it is underway. An injunction would halt the implementation and leave a gap in the modernisation of security screening. The options proposed by the applicants, including to rely on the former

Standard for those requiring only Reliability status and the 2014 Standard for those requiring other security clearances, are not feasible given that the 1994 Standard has been rescinded and the screening for Reliability status is applicable to all, as it is the starting point or base for all other security levels. The balance of convenience favours maintaining this *status quo*.

Background

[12] On October 20, 2014, the Government of Canada rescinded the 1994 Standard and launched the 2014 Standard, with a new security screening model and measures. The 2014 Standard applies to all federal departments defined in section 2 and all federal agencies included in Schedules IV and V of the *Financial Administration Act*, RSC, 1985, c F-11. Departments and agencies have until October 20, 2017 to fully implement the Standard.

[13] The Standard describes its objectives as: to ensure that government security screening practices are effective, efficient, rigorous, consistent and fair, and to enable greater transferability of security screening results between agencies and departments.

[14] The respondent provided the affidavit of Rita Whittle, Executive Director of the Security and Identity Management Division [SIDM], Chief Information Officer Branch of the Treasury Board of Canada Secretariat, with responsibility for directing the policy activities of SIDM, including all Treasury Board government security policy instruments, which includes the 2014 Standard. Ms Whittle describes the development of the Standard, the key provisions, the differences from the 1994 Standard and the screening measures which will now be used. Ms

Whittle states that she is principally responsible for the development and implementation of the 2014 Standard. She explains that the implementation process will proceed in stages and that the readiness of departments and agencies will vary to some extent.

[15] The 1994 Standard provided for two levels of Reliability status screening (Basic Reliability and Enhanced Reliability) and three levels of security clearance screening (Confidential, Secret and Top Secret). The Basic Reliability status was eliminated following the events of September 2001. Since 2002, all employees and others subject to the 1994 Standard have been required to undergo Enhanced Reliability screening (involving a name-based criminal records check and fingerprint-based check if the name-based check is inconclusive) as the first stage of screening, although their position and duties may require a higher level of screening. The minimum level of security screening from 2002 until October 2014 was Enhanced Reliability status.

[16] Under the 2014 Standard, there are three levels of Standard screening (Reliability status, Secret clearance and Top Secret clearance). Secret and Top Secret screening are for security clearances, as opposed to a status, and are required for positions with access to government classified information, assets, facilities or information technology systems. There are also two levels of Enhanced screening (Enhanced Reliability status and Enhanced Top Secret clearance).

[17] Reliability status is now the minimum level of security screening for all individuals who are employed in the federal public service and is a prerequisite for all security clearances. Enhanced Reliability status or Enhanced Top Secret clearance is required for those whose duties

involve or support security or intelligence functions, or when an individual has access to sensitive information that creates a risk of influence by criminal or ideologically-motivated persons or organizations.

[18] Obtaining and maintaining a valid security status or clearance is a condition of employment, contract, appointment or assignment. Government employees must give their informed consent to the security screening.

[19] The differences between the 1994 Standard and the 2014 Standard are summarized below. The information is derived primarily from the affidavit of Ms Whittle. The applicants portray some of the measures differently in their submissions in support of the injunction.

- Credit Checks
    - Credit checks are now mandatory for all positions and are, therefore, part of the assessment for Reliability status.
    - Credit checks were previously optional for Basic and Enhanced Reliability status and for Confidential and Secret clearance and could be conducted when duties or tasks to be performed required it or in the event of a criminal record, based on the type of offence.
    - Credit checks were previously mandatory for Top Secret clearance.

- Law Enforcement Inquiry
    - The law enforcement inquiry includes a criminal records check and a Law Enforcement Records Check [LERC].

- A criminal records check was optional before 2002 and has been mandatory for all positions since 2002.
- The Royal Canadian Mounted Police [RCMP] is responsible for conducting criminal records checks and now relies on fingerprints to do so.
- A LERC is a new component of the 2014 Standard to be conducted for Enhanced screening.
- Previously, some departments, such as the Canada Border Services Agency, RCMP, and Financial Transactions and Reports Analysis Centre of Canada, conducted LERCs as part of their screening.
- A LERC searches law enforcement databases to determine if individuals are known or suspected of being associated with organized crime, criminality or threats to national security.
- The disclosure of outstanding charges (i.e., where there is no conviction) could be done on a case-by-case basis under the 1994 Standard, depending on the type of charge and the employee's position.
- The affidavit of Brendan Heffernan, Chief Superintendent, RCMP, Canadian Criminal Real Time Identification Services indicates that disclosed criminal history information may include criminal convictions, absolute and conditional discharges with findings of guilt, and criminal charges that may be before the courts. Criminal history information about non-conviction dispositions (e.g., acquittals or withdrawals) may only be disclosed in exceptional circumstances depending on the criminal history information and its applicability to the position being screened.

- Open Source Inquiries
  - An open source inquiry involves accessing publicly available information, such as various internet sources, including social media.
  - Open source inquiries were not specifically addressed in the 1994 Standard.
  - Open source inquiries are now mandatory for screening for Enhanced Reliability status and Enhanced Top Secret clearance and optional in specific circumstances (i.e., on a case-by-case basis) for other screening, including Reliability status, when negative information is found in the security screening process.
  - Ms Whittle explains that open source information is only one of several factors considered during the screening process and the significance and relevance of the information would be considered.

- After-care
  - After-care reporting refers to the duty to report changes in circumstances and behaviour.
  - Most of these requirements were previously required under the 1994 Standard, including the requirement to attend security briefings and the requirement for those with security clearances to report changes in cohabitation or marital status.
  - The 2014 Standard requires all employees and others subject to the Standard to report changes in their criminal record status, association with criminals and significant changes in their financial situation (such as bankruptcy or unexpected wealth). Those who work in security and intelligence organizations may also be required to report changes in personal status, including marital status.

[20] The applicants seek this injunction to prohibit the implementation of particular screening measures in the Standard as they apply to employees and others requiring Reliability status until the final disposition of the application for judicial review. The screening measures the applicants take issue with are credit checks, criminal records checks to the extent that they involve fingerprinting, law enforcement inquires that involve information about outstanding charges under the *Criminal Code*, RSC, 1985, c C-46, open source inquiries and after-care reporting requirements.

[21] The applicants do not challenge the screening measures for employees who require a security clearance or Enhanced screening to perform their duties and suggest that it should be possible to carve out or exempt employees requiring only Reliability status from the new measures.

[22] The respondent highlights that Reliability status is required for all employees and is the starting point or foundation for employees who require a security clearance or Enhanced screening: i.e., Secret clearance, Top Secret and Enhanced Top Secret clearance, and Enhanced Reliability status. The respondent submits it is not possible to carve out those requiring only Reliability status from the new screening measures and that the applicants' recent amendment to narrow the scope of its motion for this injunction does not have the desired result.

The Issues

Should parts of the Applicants' Affidavit be Struck?

[23] The respondent notes that the affidavit of Martin Ranger, submitted by the applicants, contains several paragraphs that include legal opinion and argument and other paragraphs that extend beyond the personal knowledge of Mr Ranger. The respondent submits that these paragraphs should be struck. However, the respondent acknowledges that the applicants did not rely on the impugned paragraphs of the affidavit in their oral arguments.

[24] The applicants submit that the paragraphs at issue were not intended to provide legal opinion, but to provide context for the applicants' position. The applicants also note that the information included in other paragraphs, which the respondent argues is not within the affiant's personal knowledge or is hearsay or irrelevant, including the exhibits attached, has now been provided to the Court, for the most part, through other means, including as exhibits to the written cross-examination of Ms Whittle.

[25] The jurisprudence has established that striking affidavits at the preliminary stage is exceptional. However, an affidavit or parts thereof may be struck where it is vexatious or abusive, or contains conjecture, speculation or legal opinion (*Global Enterprises International Inc v Aquarius (The)*, 2001 FCT 1311, 214 FTR 269 (FCTD) [*Global Enterprises*]).

[26] In *Global Enterprises* the Court noted at para 6:

> Generally, affidavits ought not to be struck out at a preliminary stage. For the sake of efficiency, impugned affidavits should be left

> for the trial judge, who may be in a better position to assess and weigh that evidence. However, there are exceptions to this general observation, exceptions which involve special circumstance, including where an affidavit is abusive, or is clearly irrelevant, or where the Court is convinced that admissibility should be resolved at an early stage, so that the ultimate hearing might proceed in an orderly manner, or where there is conjecture, speculation or legal opinion in the affidavit. […].

[27] In the present case, the affidavit is not abusive, but it does include paragraphs which should be struck in whole or part. The context, which the applicants note as the reason for statements in the affidavit at paragraphs 12, 16 and 17, has been provided to the Court through the exhibits attached to the affidavit of Ms Whittle and through the Memoranda of Fact and Law. These paragraphs include legal opinion on the issues the Court must determine in the application for judicial review.

[28] Paragraphs 16 and 17 (describing the measures in the 2014 Standard) are struck in their entirety. Paragraph 12 is struck in part; the phrase, “much of which is unreasonable and unnecessary to achieve the objectives of its new Standard on Security Screening” is struck.

[29] Paragraphs 19, 20 and 21 are struck because this information is outside the personal knowledge of the affiant. Paragraphs 22 and 23 are also struck because this information is outside the personal knowledge of the affiant and because it relates to a different policy, not that which is the subject of this judicial review.

Should the Interlocutory Injunction be Granted?

[30] The parties agree that the test to be applied is that established by the Supreme Court of Canada in *RJR-MacDonald v Canada (Attorney General)*, [1994] 1 SCR 311, 111 DLR (4th) 385 [*RJR-MacDonald*]. This is a three-part test of which each element must be satisfied: the applicant for interlocutory relief must demonstrate that there is a serious question to be tried, meaning a question that is not frivolous or vexatious; the applicant must convince the Court that it will suffer irreparable harm if the relief is not granted; and, the balance of convenience must be found to favour the applicant.

[31] Although the test for establishing a serious issue is low, the applicants' and respondent's positions on the serious issues raised are described in some detail to provide the context for the other two elements of the three-part test.

Have the Applicants Established one or more Serious Issues?

The Applicants' Position

[32] The applicants submit that the 2014 Standard provides for the collection of personal information that was not collected under the 1994 Standard that is not necessary and that will result in an unjustified loss of privacy. The screening measures are not reasonable or proportionate despite the measures to safeguard the sensitive information.

[33] The applicants dispute the rationale advanced by Treasury Board for the 2014 Standard and submit that the goal of consistency in security screening does not make the measures

reasonable. Nor does the need to satisfy the international community, including the Five Eyes alliance (the group of countries that share intelligence in national security matters), justify the screening measures for employees at the Reliability status level. The applicants also dispute that Canadians may lose trust in public servants without new security screening measures.

[34] The applicants note that interconnected systems and networks are not new. While the internet was not firmly established in 1994, it was in 2002, yet no changes to the 1994 Standard had been made since the elimination of Basic Reliability status in 2002. The applicants argue that if there were serious concerns arising from the increased use of technology, changes would have been made before 2014.

[35] The applicants point to specific screening measures which raise serious concerns and argue that these measures violate the *Privacy Act*, RSC, 1985, c P-21, sections 7 and 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), 1982, c 11 [*Charter*] and are an abuse of discretion by the respondent.

[36] The applicants argue that a credit check is neither necessary nor effective and is not a proportionate or reasonable measure. A credit check is not relevant to assessing the loyalty and reliability of government employees who do not have access to secret or top secret information and do not have jobs relating to intelligence or security. The information obtained from a credit check is extensive, private and sensitive information, and includes a person's history of loans and mortgages, bankruptcy proposals, bankruptcy and credit report inquiries. The applicants note that

financial information is part of an individual's biographical core of information protected by the right to privacy (*R v Cole*, 2012 SCC 53 at paras 47-48, [2012] 3 SCR 34 [*Cole*]).

[37] The applicants also assert that if an employee refuses to consent to a credit check, they will not meet a condition of employment, which is to obtain Reliability status, and this would result in an administrative termination of employment.

[38] With respect to the disclosure of outstanding charges under the *Criminal Code*, the applicants submit that the 2014 Standard does not use a case-by-case approach, unlike the 1994 Standard, but seeks this information from all employees regardless of their position.

[39] In addition, fingerprints are now required through the criminal records check for Reliability status. The applicants submit that most employees will be required to use an authorized police service or private fingerprinting company to provide their fingerprints and argue that this exacerbates the aura of criminality arising from the act of fingerprinting. The applicants distinguish this from the situation of volunteers who are required to submit to a criminal records check with fingerprinting because prospective volunteers give informed consent and the measure is proportionate. The applicants' view is that name-based record checks are sufficient and the RCMP should be directed by the respondent to continue this method.

[40] The applicants also dispute the respondent's reliance on the Auditor General's recommendations regarding the RCMP's criminal record services and the use of fingerprints. The applicants submit that the Auditor General's concerns were about fingerprints for criminal

justice purposes. The applicants also dispute that the name-based records checks resulted in false positives and add that, in such cases, it is preferable to rely on fingerprints only to resolve such results, rather than as the norm.

[41] With respect to open source inquiries, the applicants submit that the search will reveal more than is reasonable or necessary for an employer. The applicants dispute the respondent's position that any breach of privacy is mitigated because only information that is relevant, reliable and attributable to the individual under review will be retained in the employee's security file.

[42] The applicants also challenge the after-care and reporting requirements that apply in the five or ten year period between security screenings. The applicants note this will have a "chilling" effect despite that only information that raises a concern about loyalty or reliability would be noted. The applicants add that the scope of reporting is too broad; only those requiring higher levels of security should be required to report a change in their criminal record or their association with criminals, and there is no reason for anyone to report changes in their wealth or marital status.

[43] The applicants submit that even if the information is only provided to or shared with qualified personnel, this does not respond to the breach of privacy because the information should not be accessed in the first place.

[44] The applicants argue that these measures raise several serious legal issues that should be addressed in the application for judicial review.

Breach of the Privacy Act

[45] The applicants submit that the Standard does not comply with the *Privacy Act*, particularly section 4, which provides that personal information shall not be collected unless it relates directly to an operating program or activity of the institution.

[46] The jurisprudence establishes that providing an individual with control over his or her personal information is connected to individual autonomy, dignity and privacy, and that privacy legislation is quasi-constitutional, as privacy plays a fundamental role in the preservation of a free and democratic society (*Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401*, 2013 SCC 62 at paras 19, 21-22, 24, [2013] 3 SCR 733). The applicants submit that the unreasonable screening measures deprive employees of this control.

[47] The applicants argue that the *Privacy Act* can be an independent source of legal rights (and note, for example, *Bernard v Canada (Attorney General)*, 2014 SCC 13 at paras 30-33, [2014] 1 SCR 227 [*Bernard*]; *Zarzour v Canada*, [2000] FCJ No 2070 (QL) at paras 23-29, 196 FTR 320 (FCA) [*Zarzour*]).

[48] Although section 5.2.3 of the Standard expressly requires compliance with the *Privacy Act*, this does not mean that the Standard does comply. The applicants submit that they have a right to seek a declaration that Treasury Board has breached or failed to comply with the *Privacy Act*.

Breach of Section 8 of the Charter

[49] The applicants submit that the exercise of discretion in adopting the Standard must be carried out in a manner that conforms to the *Charter* (*Canada (Attorney General) v PHS Community Services Society*, 2011 SCC 44 at para 117, [2011] 3 SCR 134).

[50] The applicants argue that the screening measures in the Standard violate the reasonable expectation of privacy of employees. Employees should not have to trade off their privacy rights to become employees.

[51] Section 8 prohibits unreasonable search and seizure and applies in the administrative law context (*R v McKinlay Transport Ltd*, [1990] 1 SCR 627 at 647, 72 OR (2d) 798 [*McKinlay*]; *Gillies (Litigation Guardian of) v Toronto School Board*, 2015 ONSC 1038, 125 OR (3d) 17). The applicants argue that Treasury Board, acting as an employer, is carrying out a search under section 8 by requiring and collecting personal information.

[52] The applicants submit that the reasonableness of the search must take into account the privacy interests at stake. Section 8 "seek[s] to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of an individual" (*R v Tessling*, 2004 SCC 67 at para 25, [2004] 3 SCR 432 [*Tessling*], citing *R v Plant*, [1993] 3 SCR 281 at 293, [1993] 8 WWR 287). Informational privacy is included in the definition of privacy (*Tessling* at para 23).

[53] The applicants emphasize that the Supreme Court of Canada has clearly established that privacy is a matter of reasonable expectations (*Cole* at para 35) and that even a diminished expectation of privacy can be a reasonable expectation of privacy (*Cole* at para 9).

[54] The applicants submit that the screening measures in the Standard would require employees to reveal details of their lifestyle and personal choices, including contacts with police, financial information, ideology, conduct and associations, and that this amounts to an unreasonable search.

[55] The applicants did not pursue the argument that the Standard violates the privacy protections under section 7 of the *Charter* and that this raises a serious issue.

Abuse of Discretion and Authority

[56] Abuse of discretion is a basis for Courts to review the exercise of administrative discretion on the grounds of legality, reasonableness and fairness (*Canada (Attorney General) v TeleZone Inc*, 2010 SCC 62 at para 24, [2010] 3 SCR 585; *Dunsmuir v New Brunswick*, 2008 SCC 9 at para 28, [2008] 1 SCR 190).

[57] The applicants submit that the Standard and its screening measures violate the common law of the workplace and amount to an abuse of discretion and authority by Treasury Board. Treasury Board must justify the infringement of an employee's legitimate right to privacy with clear and compelling evidence and has not done so.

[58] The applicants rely on several arbitration decisions to support their argument that the common law of the workplace requires that the employer not exercise its discretion in a manner that is overly privacy invasive, including *Vancouver (City) v Canadian Union of Public Employees Local 15*, [2007] BCCAAA No 216, 91 CLAS 298; *Winnipeg (City) v Canadian Union of Public Employees Local 500*, [2002] MGAD No 21; *Canada Post Corp v Canadian Union of Postal Workers (CUPW 730-85-00037)*, [1988] CLAD No 12, 34 LAC (3d) 392; and, *Ottawa (City) v Ottawa Professional Firefighters Assn*, [2007] OLAA No 731, 169 LAC (4th) 84.

[59] The applicants also note that the Supreme Court of Canada has confirmed, in the context of alcohol and drug testing in the workplace, that employers can only impose rules where "the need for the rule outweighs the harmful impact on employees' privacy rights" (*Communications, Energy and Paperworkers Union of Canada, Local 30 v Irving Pulp & Paper, Ltd*, 2013 SCC 34 at para 4, [2013] 2 SCR 458).

The Respondent's Submissions

[60] The respondent notes that the determination whether a serious issue has been raised and the other aspects of the three-part test must be considered in the appropriate context.

Context

[61] The respondent notes that security screening began in the 1940s. Cabinet Directives established in the 1950s and 60s provided guidance until the issuance of the Treasury Board

Policy on Government Security in 1986 (1986 Policy) and the 1994 Standard. The 1994 Standard was rescinded in 2014. The 2014 Standard reflects modernisation; some of the same screening measures remain, while others have been modified or are new.

[62] The 2014 Standard is essential to maintain trust between the government and citizens and between the government and other stakeholders, including foreign governments.

[63] The level of security screening under the Standard will depend on the sensitivity of the information an employee will have access to; however, all employees must be screened for Reliability status. Reliability status underpins all other security levels.

[64] The respondent notes that those with Reliability status have access to a wide range of information, information technology systems and unescorted access to facilities. Those with Reliability status perform duties and activities which could give them access to a great deal of information that is provided and retained for a range of government programs. It is essential to ensure that employees responsible for programs and services can be trusted with the information they have access to.

[65] The affidavit of Ms Whittle describes the need for the new Standard, including the evolving nature of threats to the security of Canada, particularly since 2001, and the need to provide assurances to the Five Eyes intelligence-sharing community that Canada’s security policy is analogous to the policies of other members of the community.

[66] The Standard also reflects the evolution in the workplace, including open work spaces, significant reliance on technology, the interconnected networks that employees have access to and the increased use of social media. In addition, the establishment of Shared Services Canada, which merges many services for government departments, results in data being accessed by more employees.

[67] Ms Whittle also provided exhibits indicating that the development of the Standard dates back to a 2003 survey regarding screening of personnel conducted by the Privy Council Office and includes the results of a subsequent task force, which made recommendations to modify the security screening regime.

[68] The respondent notes that there was no oral cross-examination of Ms Whittle; however, written answers and exhibits were provided. Her evidence of the development of the Standard and the need it meets is, therefore, uncontradicted.

No Serious Issue

[69] The respondent argues that the applicants have not raised any serious issue.

[70] The respondent highlights that the information provided by an employee is not accessible to anyone other than the qualified, trained personnel responsible for security in a department, for example, the Departmental Security Officer, who is tasked with conducting the assessment. These professionals do not disclose the information gathered to the manager or anyone else.

[71] The respondent notes that the applicants have misconstrued some of the screening measures and their applicability.

[72] Credit checks are not new measures, as these were included in the 1994 Standard, but are now mandatory. The credit check is done by a credit reporting agency, but the agency will "mask" the inquiry so it will not be apparent that the inquiry was made.

[73] The respondent contests the applicants' assertion that refusal to consent to a credit check would result in an administrative termination of employment. The policy simply provides that the cancellation of a person's security status or clearance could result in termination of employment; however, there would be opportunities for explanation and several factors would be considered to determine whether the security status or clearance could be granted. In addition, there are redress mechanisms.

[74] The respondent notes that the 2014 Standard requires a criminal records check, but the Standard does not specify a method and does not require that criminal records checks be conducted by fingerprinting. The RCMP is responsible for performing criminal records checks under the Standard and has adopted, effective July 2015, a fully electronic, fingerprint based, criminal records check model to identify the person and the record. The affidavit of Chief Superintendent Heffernan explains the reasons for doing so, including the recommendations of the Auditor General that fingerprints are an international best practice, their accuracy and their expediency. The respondent notes that the RCMP's decision to require fingerprinting for criminal records checks is not at issue in the judicial review.

[75] In addition, the requirement for fingerprinting by a third party is not new; both the 1986 Policy and the 1994 Standard provided for fingerprinting in some circumstances as part of the criminal records check and, when required, fingerprints could be taken at an RCMP office or local police station.

[76] The respondent adds that the Auditor General's 2000 and 2004 reports do in fact refer to fingerprinting in the employment security screening context.

[77] With respect to the disclosure of outstanding criminal charges, the respondent submits that the applicants have misconstrued the requirements; the 2014 Standard does not require disclosure. The RCMP would only disclose non-conviction information as part of a criminal records check in exceptional circumstances, as explained in the affidavit of Chief Superintendent Heffernan. The respondent notes that this evidence is uncontradicted.

[78] The release of criminal records information under the Standard is governed by the *Criminal Records Act*, RSC, 1985, c C-47, the *Youth Criminal Justice Act*, SC 2002, c 1), the *Privacy Act*, the Criminal Code and directives from the Minister of Public Safety. The respondent also notes that a LERC is only required for Enhanced screening.

[79] With respect to open source inquiries, the respondent submits that such inquiries could have been undertaken previously as there was no prohibition and the information is publicly available. Now open source inquiries are specifically addressed, but are mandatory only for Enhanced screening and are optional for screening for Reliability status, as part of after-care or

for cause. The respondent adds that if there is a risk of behaviour or association with others that may pose a security risk or make a person vulnerable, it would be risky not to check the publicly available information.

[80] After-care reporting is intended to ensure that in the ten year period between screenings there is no change in the employee's ability to do their job and perform their duties in a reliable and trustworthy manner. After-care was part of the 1994 Standard. The 2014 Standard seeks to standardize the measure.

[81] The respondent submits that the applicants have not raised a serious issue; the Standard and the screening measures at issue do not violate the *Privacy Act* or *Charter* and do not reflect an abuse of discretion.

Breach of the Privacy Act

[82] The respondent notes that the Standard specifically requires compliance with the *Privacy Act* and there is no evidence that it violates the *Privacy Act*.

[83] Recourse for a breach of the *Privacy Act* can be sought by filing a complaint to the Privacy Commissioner with respect to the collection, retention, disposal, use or disclosure of personal information held by a government institution (*Privacy Act* at para 29(1)(h)). The only recourse to the Federal Court provided under the *Privacy Act* is for individuals who are refused access to their information and who have made a complaint with the Privacy Commissioner (section 41).

[84] The respondent submits that the jurisprudence relied on by the applicants to support their argument that the *Privacy Act* can be an independent source of legal rights and that declaratory relief against alleged violations of privacy rights can be granted arose from different circumstances and focussed on how government institutions handled the information in their possession.

[85] The respondent agrees that section 4 of the *Privacy Act* provides that personal information should not be collected unless it relates to an operating program and submits that the Standard is such a program. The Standard sets out how personal information will be handled and includes safeguards.

[86] The respondent refers to Appendix C of the Standard which describes the collection, use, disclosure, retention and disposal of personal information for the purpose of security screening. These activities must be carried out in compliance with the *Privacy Act* and with other applicable legislation, policies, directives, standards and guidelines.

[87] The respondent disputes the applicants' argument that simply collecting the information constitutes a violation of an employee's privacy.

Section 8 of the Charter

[88] The respondent submits that although the screening measures may be more rigorous than they were previously, this does not make them unreasonable (*Reference re Marine*

Transportation Security Regulations, 2009 FCA 234 at para 66, 395 NR 1 [*Marine Transportation Reference*]).

[89] The Federal Court of Appeal determined that screening measures analogous to those at issue were not overly intrusive and were not unreasonable in *Marine Transportation Reference*. Given that similar considerations exist in the present case, the respondent submits that there is no serious issue raised with respect to section 8, as it has already been decided.

[90] The Standard demonstrates a balance between the privacy protections of the *Charter* and the legitimate objective of the government to maintain the integrity of its information, assets and facilities, which enables the government to deliver programs and services to Canadians and to advance Canada's interests (including national security). The Standard affects the applicants' right to privacy as little as reasonably possible to achieve this objective.

[91] The respondent notes that context determines whether a reasonable expectation of privacy is held (*British Columbia Securities Commission v Branch*, [1995] 2 SCR 3 at para 51, 123 DLR (4th) 462 [*Branch*]; *McKinlay* at 646; *R v Jarvis*, 2002 SCC 73 at paras 63, 69-72, [2002] 3 SCR 757) and what is reasonable will differ in the criminal and administrative law contexts (*Branch* at para 52).

Section 7 of the Charter

[92] The respondent submits that there is no serious issue to be tried regarding a breach of section 7 of the *Charter* and notes that the applicants did not pursue this argument. In *Marine*

Transportation Reference at para 44, the Federal Court of Appeal found that protection from unreasonable search is specifically provided for under section 8 and that such issues are therefore not appropriately considered under section 7.

Abuse of Discretion and Authority

[93] The respondent characterizes the applicants' allegations of abuse of discretion as bald and unsupported by any evidence or arguments.

[94] Treasury Board is the employer and acts pursuant to the *Financial Administration Act*, but its role extends beyond human resources management. It has the authority to make policy regarding the administration of the government and did not abuse its discretion in doing so. The respondent again notes that the evidence of Ms Whittle explains the development of and rationale for the Standard and is uncontradicted.

[95] The respondent submits that there is a clear rationale for the Standard that is defensible in respect of the facts and law and, therefore, it meets the reasonableness standard of review.

[96] The respondent distinguishes the arbitration decisions cited by the applicants because they did not involve employment with the government and, in many of the cases, the policies were highly intrusive and involved physical invasions of the employees' bodily integrity or property. The 2014 Standard does not include such measures.

The Applicants have Established one or more Serious Issues

[97] As noted above, the first stage of the *RJR-MacDonald* test is whether there is a serious issue to be tried, as described at 348:

> At the first stage, an applicant for interlocutory relief in a *Charter* case must demonstrate a serious question to be tried. Whether the test has been satisfied should be determined by a motions judge on the basis of common sense and an extremely limited review of the case on the merits. The fact that an appellate court has granted leave in the main action is, of course, a relevant and weighty consideration, as is any judgment on the merits which has been rendered, although neither is necessarily conclusive of the matter. A motions court should only go beyond a preliminary investigation into the merits when the result of the interlocutory motion will in effect amount to a final determination of the action, or when the constitutionality of a challenged statute can be determined as a pure question of law. Instances of this sort will be exceedingly rare. Unless the case on the merits is frivolous or vexatious, or the constitutionality of the statute is a pure question of law, a judge on a motion for relief must, as a general rule, consider the second and third stages of the *Metropolitan Stores* test.

[98] In the present case, a stay in the implementation of the Standard will not necessarily result in the Standard never coming into force, but it would halt its implementation now and delay it pending final determination of the judicial review. Therefore, the result of this motion will not amount to a final determination of the issues. The Court is not required to go beyond a preliminary investigation of the merits, as this is the role of the judge who will determine the application for judicial review.

[99] The applicants have raised three issues. Based on a preliminary assessment, none of the issues can be found to be frivolous or vexatious, although they may not ultimately be found to be meritorious on judicial review.

Breach of the Privacy Act

[100] The Standard is required to comply with the *Privacy Act* in its application and employees would be able to make a complaint to the Privacy Commissioner with respect to particular instances of non-compliance. The complaint process would not address whether the Standard as a whole complies with the *Privacy Act*, particularly given the uncertainty as to whether the Privacy Impact Analysis was completed before the Standard was implemented.

[101] As noted by the respondent, the jurisprudence relied on by the applicants to support their argument that declaratory relief can be granted pursuant to the *Privacy Act* is not persuasive. In *Zarzour*, the Court of Appeal noted the obligations on the Parole Board to respect the information it held, in accordance with the *Privacy Act*, and in *Bernard* the focus was on whether the information held by the union was consistent with the purpose for which it was obtained.

[102] Regardless, the issue of whether the 2014 Standard complies with the *Privacy Act* should be fully canvassed on the judicial review.

Section 8

[103] In *Harper v Canada (Attorney General)*, 2000 SCC 57, [2000] 2 SCR 764 [*Harper*], the Supreme Court of Canada applied the three-part test from *RJR-MacDonald* and commented on the serious issue branch at para 4:

> […] Without prejudging the appeal, we are satisfied there is a serious issue to be tried. The issue is no less than the constitutionality of provisions of the electoral law passed by the Parliament of Canada which no court has held to be invalid. This is

> a serious issue not only because the constitutionality of the provisions is challenged, but because it is common ground that the determination of the constitutionality will turn on the application of s. 1 of the Charter, which is always a complex factual and legal analysis. […]

[104] Similarly in the present case, the determination as to whether the screening measures in the Standard violate section 8 requires a more detailed analysis.

[105] Section 8 of the *Charter* provides that "everyone has the right to be secure against unreasonable search or seizure."

[106] The applicants assert that their reasonable expectation of privacy is infringed by the Standard. However, this determination requires more than simply the assertion of the applicants that there is a reasonable expectation of privacy in all the information sought and that the requirement to provide this information is not justified. A subjective expectation of privacy is not determinative of a reasonable expectation of privacy. What is reasonable will be informed by the context and the balancing of the competing interests at play.

[107] The applicants relied on *McKinlay* with respect to the subjective expectation of privacy. In *McKinlay*, the Court found that the requirement to comply with a demand to provide documents pursuant to the *Income Tax Act*, RSC, 1985, c 1 (5th Supp) constituted a seizure because it infringed the reasonable expectation of privacy of those required to comply, but went on to find that there was no breach of section 8.

[108] The Court noted at 645 that "individuals have different expectations of privacy in different contexts and with regard to different types of information and documents" and, therefore, what is reasonable will depend on the context. The Court noted that only unreasonable searches infringe section 8.

[109] In *Cole*, the Supreme Court of Canada held that "[i]f the claimant has a reasonable expectation of privacy, s. 8 is engaged, and the court must then determine whether the search or seizure was reasonable" (at para 36).

[110] However, whether a person has a reasonable expectation of privacy depends on the "totality of the circumstances" (at para 39). The Court noted the considerations at para 40:

> The "totality of the circumstances" test is one of substance, not of form. Four lines of inquiry guide the application of the test: (1) an examination of the subject matter of the alleged search; (2) a determination as to whether the claimant had a direct interest in the subject matter; (3) an inquiry into whether the claimant had a subjective expectation of privacy in the subject matter; and (4) an assessment as to whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances (*Tessling*, at para. 32; *Patrick*, at para. 27). I will discuss each in turn.

[111] In assessing whether a subjective expectation of privacy is objectively reasonable, the Court in *Cole* noted that the closer the subject matter of the search lies to a biographical core of information, such as information that reveals details of the lifestyle and personal choices of the person, the more this will favour a reasonable expectation of privacy (at paras 44-46).

[112] Although the information required pursuant to the screening measures can be characterized as part of the biographical core of personal information that one may wish to protect, that is not determinative of the reasonableness of the "search". The determination of whether the search is reasonable is more complex and will involve a balancing of factors (*Harper* at para 4).

[113] The Court on the judicial review will determine the scope of the reasonable expectation of privacy in the relevant context, whether the search was authorized and whether the policy is reasonable, which includes balancing the privacy interests and the government's objectives in adopting the 2014 Standard.

[114] *Marine Transportation Reference* considered screening measures, similar to some of those in the 2014 Standard, and concluded that the information required to be gathered was not overly intrusive and that, considering the purpose of the measures and the risks addressed, it was not an unreasonable search and did not violate section 8 (at para 69).

[115] While *Marine Transportation Reference* will be very relevant to the determination of the section 8 issue on judicial review, I do not share the respondent's view that it has determined the serious issue raised by the applicants once and for all. The 2014 Standard and its broad application differs from the screening measures applicable to ports' employees who worked in an environment requiring heightened security at all times and whose concerns extended to the sharing of their information with others. In *Marine Transportation Reference*, the Court of Appeal noted the considerations in the balancing of employees' interests in privacy and the

public interest served by the regulations which imposed the security measures. These include contextual factors: the strength of the privacy interests at stake (at para 50); the manner of the search (at para 51); that administrative searches are less intrusive than those conducted for a criminal investigation (at para 52); and how pressing the public interest is and to what extent the information sought is likely to further the intended purpose (at para 53). The same or similar considerations would be part of the balancing in the present case.

[116] With respect to section 7 of the *Charter*, I agree with the respondent that, following *Marine Transportation Reference*, there is no serious issue to be tried on whether there is an independent section 7 claim (and the applicants appear to have abandoned this argument).

Abuse of Discretion and Authority

[117] The respondent's rationale for the development of the Standard and the need that it meets has been explained in the affidavit of Ms Whittle and is uncontradicted. The respondent again notes that the Standard responds, among other things, to a survey conducted in 2003 and a later task force, and that consultations were undertaken in the process of developing the Standard.

[118] Although the applicants simply assert that the Standard is an abuse of discretion or authority, and provide no evidence to support this assertion, the issue cannot be characterized as frivolous. The applicants should have an opportunity to fully advance their argument on judicial review.

[119] As noted by the applicants, the threshold to establish a serious issue is low and unless the case on the merits is frivolous or vexatious, the second and third elements of the test will be determinative.

Have the Applicants Established Irreparable Harm?

The Applicants' Submissions

[120] The applicants submit that if the injunction is not granted and the judicial review is successful, employees of the federal government will suffer irreparable harm. They are required to consent to provide privacy-invasive information as a condition of their continued employment. The applicants submit that their consent cannot be considered voluntary because a valid security clearance is a condition of employment. If an employee refuses to consent, they will not be considered for the position, or in context of a renewal or update of their security status, a cancellation of their security clearance would lead to administrative termination.

[121] The applicants submit that privacy violations are inherently harmful and this harm would be irreparable because once lost, privacy cannot be regained. As a result, the harm must be prevented. The applicants note that in *R v Dyment*, [1988] 2 SCR 417 at 430, 55 DLR (4th) 503, the Supreme Court of Canada held that "if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated."

[122] The applicants point to *Bisaillon v Canada*, [1999] FCJ No 898 (QL) at para 34, 251 NR 225 (FCA), where the Federal Court of Appeal found that the loss of privacy in turning over

tax documents to Revenue Canada pending the final outcome of a challenge to Revenue Canada's right to access those documents was a loss of privacy constituting irreparable harm. In the present case, turning over personal information for security screening purposes would be a loss of privacy constituting irreparable harm.

[123] The applicants also point to the decision of the Supreme Court of Canada in *143471 Canada Inc v Quebec (Attorney General)*, [1994] 2 SCR 339, 31 CR (4th) 120 [*143471 Canada*], where the Court found that if the constitutional allegations turned out to be correct, then the loss of privacy itself would constitute irreparable harm (at 380). The applicants argue that this principle applies regardless of the fact that the search at issue in *143471 Canada* was intrusive; the intrusiveness of the search was noted by the Court only as additional factor.

[124] The applicants argue that if they are correct and the 2014 Standard violates the *Charter*, irreparable harm is established.

[125] The applicants also refer to several cases where courts and arbitrators have granted interim injunctions to protect the privacy rights of employees pending the final outcome of a challenge to a policy of an employer.

[126] The applicants argue that *International Longshore and Warehouse Union, Canada v Canada (Attorney General)*, 2008 FCA 3, 371 NR 357 [*Longshore*] (the interlocutory order denying a stay of the legislation in the *Marine Transportation Reference* proceedings) is

distinguishable. Although the Court found no evidence of irreparable harm, in that case the issue was discipline and loss of jobs, which are compensable (at paras 23-24, 35).

[127] In the present case, the applicants note that their concern is not about the implications for employment but simply the harm from the breach of privacy itself.

[128] If the injunction is not granted, employees will be required to submit to credit checks and fingerprinting, and will have to continually advise the employer of their associations with particular people or their personal status. This engages very real privacy interests of public servants. The applicants argue that there is no remedy to repair this unauthorized invasion of privacy.

[129] The applicants dispute the respondent's argument that irreparable harm has not been established and that the affidavit of Mr Ranger does not provide any such evidence. The applicants point out that the Standard states that it will be implemented. Fingerprinting measures already commenced on July 1, 2015. Clearly union members will be subjected to the screening measures. The fact that other measures have not yet been implemented does not make the application for judicial review or the motion for an injunction speculative.

[130] In response to questions from the Court about why there is no evidence from a member of the union who will be subject to the new screening measures describing the irreparable harm that person will suffer before the application for judicial review is determined, the applicants advised that it would have been possible to provide such evidence, but that common sense can be relied

on to establish that, out of 35,000 members who are required to have their security clearance renewed every ten years, some or many will be subjected to the Standard now or in the near future. They are also all required to report changes to personal circumstances and are subject to ongoing monitoring. The applicants add that Mr Aubry would either be subject to the Standard in this period for the purpose of renewal of his status or due to the ongoing monitoring and reporting requirements, such as the open source inquiries or mandatory reporting of changes to his personal circumstances. The applicants submit that it is obvious that Mr Aubry and others will suffer irreparable harm.

[131] The applicants add that it would be unreasonable to require the union to set out which of its members will undergo security screening before the judicial review is decided. The applicants claim that the union has no record of the security status of each of its members, but suggest that only 10% would require more than Reliability status. The applicants caution that if the Court finds that there should be actual evidence of irreparable harm, it will file a new application and bring another motion for an injunction in the context of an individual member who is required to be screened.

[132] The applicants also argue that it is not necessary for them to establish actual harm resulting from the screening measures. In the applicants' words, the employer should not be "nosing around." The applicants' affidavit does not need to address actual harm because irreparable harm arises automatically from the application of the Standard and the search itself. The applicants question what would be added by providing an affidavit of an employee who will be screened.

The Respondent's Submissions

[133] The respondent acknowledges that it is the nature, not the magnitude, of the harm that is relevant (*RJR-MacDonald* at 348). The irreparable harm to the party seeking the injunction must be established, i.e., to the applicants, and the harm at issue must result from the implementation of this policy, i.e., the 2014 Standard. In addition, specific and concrete evidence of actual harm must be adduced (*Glooscap Heritage Society v Canada (Minister of National Revenue)*, 2012 FCA 255 at para 31, 440 NR 232 [*Glooscap*]).

[134] The respondent submits that in the present case, no evidence of irreparable harm has been provided. The applicants only assert a general loss of privacy arising from the implementation of the Standard. A general assertion cannot establish irreparable harm (*Gateway City Church v Canada (National Revenue)*, 2013 FCA 126 at para 15, 445 NR 360 [*Gateway*]). Allegations of speculative invasions of privacy do not independently establish irreparable harm (*Longshor*e at paras 26, 33).

[135] The respondent notes that the Standard also provides that security screening is to be conducted every five or ten years, depending on the level of clearance; however, the applicants provided no evidence that union members will undergo security screening between now and the determination of the application for judicial review. Consequently, the Court cannot conclude that the applicants will suffer irreparable harm before the hearing on the merits.

[136] The respondent clarifies that its position is not that the applicants must account for the security screening status of each union member; it is rather that the applicants must provide

evidence of irreparable harm with respect to some member(s). The respondent notes that the affidavit of Mr Ranger does not address the irreparable harm alleged. It only refers to a negative impact on employment. There is no affidavit from the applicant, Mr Aubry, indicating the harm he will suffer, if any, nor is there an affidavit from any other member of the union.

[137] The respondent submits that *143471 Canada*, relied on by the applicants, does not establish as a general proposition that a loss of privacy necessarily constitutes irreparable harm. In that case, the irreparable harm flowed from the manner in which the privacy interest was compromised, which involved searches of private homes and seizure of documents. The Federal Court of Appeal has considered *143471 Canada* in other more recent cases. In *Canada (Attorney General) v Canada (Information Commissioner)*, 2001 FCA 26 at para 22, 12 CPR (4th) 492 [*Information Commissioner*], the Court of Appeal noted that a different conclusion may have been reached if the information had been obtained by less intrusive means.

[138] The respondent notes that the 2014 Standard involves obtaining information only for security screening purposes and does not involve bodily searches or forced disclosure of documents, as the cases cited by the applicants did.

[139] In *Marine Transportation Reference*, the Federal Court of Appeal rejected a union's argument that new security screening measures, which required employees to provide similar information to that required by the 2014 Standard, infringed the employees' privacy rights. The Court of Appeal found that demands for personal information and fingerprints are among the least intrusive forms of search (at para 61).

[140] Similarly, the Supreme Court has recognized that fingerprinting is "insubstantial," "leaves no lasting impression" and may be legitimately used for a wide variety of purposes (*R v Rodgers*, 2006 SCC 15 at paras 41, 51, [2006] 1 SCR 554, citing *R v Beare*, [1988] 2 SCR 387 at 413, 55 DLR (4th) 481). The respondent submits that the same conclusion of minimal intrusiveness applies in the present case.

[141] The respondent submits that the mere collection of information does not establish a violation of privacy interests and that the applicants' allegations that their right to privacy will be breached once the information is collected is speculative (*Information Commissioner* at para 21).

[142] Many aspects of the 2014 Standard, such as the guidelines on the financial assessment questionnaire, and on the security questionnaire and interviews, have not been finalized. The respondent disputes the applicants' assumption that these guidelines will violate their privacy rights rather than protect them. There are many checks and balances in the Standard to protect the information provided.

[143] The respondent also points to its adoption of best practices for the collection, use and disposal of personal information obtained under the Standard. Only authorized and qualified personnel have access to the information on a need-to-know basis. The respondent reiterates that credit checks will be masked and will not affect the employee's credit rating, fingerprints will be automatically destroyed, information about outstanding charges will be disclosed only in exceptional circumstances, open source inquiries are of already public information, and the information gathered by an open source inquiry is used only to assess reliability and loyalty and

would be reviewed only by the Security Officer who is qualified and trained. The Standard also includes redress and review mechanisms for addressing errors or concerns that may arise in a security screening. In a similar context, in *Marine Transportation Reference,* the Federal Court of Appeal found that these mechanisms appropriately address concerns about possible errors. The respondent argues that these measures undermine the applicants' claims regarding irreparable harm.

[144] The respondent argues that the applicants have failed to provide concrete, non-speculative evidence that the alleged harm will occur before the application is heard. Without any evidence from a member of the union who has or will be required to undergo screening for Reliability status, the respondent is denied the opportunity to test the evidence and probe the alleged harm.

[145] The respondent also adds that the applicants cannot simply assert that they will bring another motion with the necessary evidence of irreparable harm. The applicants should have "put their best foot forward" in this motion.

The Applicants Have Not Established Irreparable Harm

[146] In *RJR-MacDonald,* the Supreme Court of Canada described irreparable harm at 348:

> At the second stage the applicant must convince the court that it will suffer irreparable harm if the relief is not granted. `Irreparable' refers to the nature of the harm rather than its magnitude. In Charter cases, even quantifiable financial loss relied upon by an applicant may be considered irreparable harm so long as it is

> unclear that such loss could be recovered at the time of a decision on the merits.

[147] The applicants' position remains that the mere provision of information is a loss of privacy which cannot be restored and that this is harmful on its own, regardless of the rationale for the screening measures and the protections in place to safeguard that information.

[148] The applicants rely on *143471 Canada* to support their argument that if they are ultimately successful on judicial review and the Court agrees that aspects of the Standard violate section 8, then the loss of their privacy now (before the issue is ultimately decided) constitutes irreparable harm.

[149] In *143471 Canada*, decided shortly after *RJR-MacDonald*, the Supreme Court of Canada applied the three-part test in the context of searches and seizures of tax information, which extended to searches of private homes. On the issue of irreparable harm, Justice Cory, writing for the majority in this 4:3 decision, stated at page 380:

> The purpose of an interlocutory stay is to preserve the rights of applicants (the respondents before this Court) pending a final determination of a legal question which will affect those rights. Here, the respondents seek not the return of their documents, but simply the maintenance of the orders that they be held by the court pending the determination of this issue. If it is found that the respondents are correct and that the searches and seizures were unconstitutional, then the privacy right will have effectively been lost as a result of the unconstitutional provisions of the Act. Small as it may be, there is such a privacy interest. If it transpires that the respondents are correct in their constitutional contention, then I would think that the loss of that privacy interest would, in itself, constitute irreparable harm.
>
> [Emphasis added]

[150] However, Justice Cory said more than this and the applicants' reliance on only this paragraph does not, in my view, establish that the possibility that an allegation of a breach of section 8 may be resolved in favour of the applicants is sufficient to establish irreparable harm, without any other evidence of such harm.

[151] In the following paragraph of *143471 Canada*, at page 380, Justice Cory added: "Yet there is another aspect which I consider to be far more significant in this case. Namely, that the documents were obtained by means of intrusive searches of residential and business premises."

[152] While the applicants characterize this as simply an additional factor which does not detract from the principle set out above, the preceding and following paragraphs make it clear that this was not simply an additional consideration, but a consideration which influenced Justice Cory's ultimate conclusion. His comment that "I would think that the loss of that privacy interest would, in itself, constitute irreparable harm" is slightly tentative. In the following paragraph, Justice Cory notes the intrusiveness of the searches, including in private homes. The conclusion, at page 381, confirms that the nature of the search was more than an additional factor, and was a significant factor in finding irreparable harm on the facts of that case:

> The constitutionality of ss. 40 and 40.1 of *An Act respecting the Ministère du Revenu* will be determined in the principal applications to quash the warrants. Should those sections eventually be found to be unconstitutional, then the searches and seizures will have violated the privacy interest of the respondents in their homes and offices. The government will, without authority, have entered the premises and searched for and seized the documents. Thus the government will have had the continuing possession of the documents in the absence of any authority and in violation of the *Charter*. This, it seems to me, would constitute irreparable damage to the respondents.

[153] The dissenting judges took a different view regarding the finding of irreparable harm. Justice La Forest commented at page 361:

> However, the present case can be distinguished from *Dyment*, where the respondent was challenging the seizure of a bodily fluid without prior authorization. The respondents are objecting here to the examination by the tax authorities of the contents of business documents the seizure of which was previously authorized. The existence of irreparable harm cannot be inferred simply because a breach of a right protected by the Charter is alleged or because the main proceeding itself involves the infringement of an entrenched right. In the present case not only have the courts not yet made a final ruling on whether the searches are unreasonable, but the Quebec Superior Court dismissed the motion in evocation, certiorari and mandamus in the *143471 Canada Inc.* case. It seems wrong to conclude as a matter of principle that the right to privacy must in all circumstances take priority over any other interest, for example over giving effect to legislation adopted in the public interest. Both the right and the alleged infringement must be placed in context: see *United States of America v. Cotroni*, [1989] 1 S.C.R. 1469, and *Edmonton Journal v. Alberta (Attorney General)*, [1989] 2 S.C.R. 1326. Accordingly, before concluding that the harm is "irreparable", as required by the second criterion, the existence and extent of the harm must be determined, something which the Court of Appeal seems to have failed to do in the case at bar since it simply said that the seized documents might [translation] "contain personal items of information and so contravene the protection of privacy guaranteed by law" (p. 45 R.D.F.Q.).
>
> [Emphasis added]

[154] The Federal Court of Appeal has specifically commented on *143471 Canada* and has found that irreparable harm must be established independently of arguments regarding the constitutionality of the measure at issue and cannot be inferred based on a potential *Charter* breach that has yet to be determined. This view, which favours those of the dissenting justices in *143471 Canada*, has been confirmed in several decisions.

[155] In *Information Commissioner*, the Court of Appeal noted (at paras 12, 22) that irreparable harm cannot be speculative and that *143471 Canada* was decided in the context of an intrusive search:

> [12] First, the fact that irreparable harm may arguably arise does not establish irreparable harm. What the respondents had to prove, on a balance of probabilities, is that irreparable harm would result from compliance with the subpoenas issued on behalf of the Commissioner (*Manitoba (Attorney General) v. Metropolitan Stores (MTS) Ltd.*, [1987] 1 S.C.R. 110 at para. 35). The alleged harm may not be speculative or hypothetical (*Imperial Chemical Industries PLC v. Apotex Inc.*, [1990] 1 F.C. 211 (C.A.)).
>
> […]
>
> [22] The decision of the Supreme Court in *14371 Canada Inc. v. Québec [A.G.]*, [1994] 2 S.C.R. 339 [sic] brought to our attention by the respondents rested on an entirely different set of facts. It dealt with intrusive searches of residential and business premises by the tax authorities under constitutionally suspect statutory authority. The Court in its reasons noted on more than one occasion that searches of private property are far more intrusive than a demand for production of documents, thereby giving rise to a greater need for the protection of the privacy interests of those concerned (see pages 380, 381 and 382). That is the context in which the majority concluded that irreparable harm would result if the seized documents were reviewed by the tax authorities, pending the determination of the constitutional validity of the seizure. <u>It is clear that a different conclusion would have been reached if the information in issue had been obtained by less intrusive means</u>.
>
> [Emphasis added]

[156] In *Groupe Archambault Inc v Cmrra/Sodrac Inc*, 2005 FCA 330, 357 NR 131, the Court of Appeal acknowledged its preference for the views of the dissenting justices in *143471 Canada*. Similar to the arguments in the present case, the applicants relied on *143471 Canad*a to argue that the infringement of its constitutional right to privacy was irreparable harm in and of

itself. The Court of Appeal referred to its own decision in *Information Commissioner* and concluded at para 16:

> In my opinion, the mere allegation of an infringement of section 8 is insufficient to establish irreparable harm. This Court's interpretation of *143471 Canada Inc. Canada (Attorney General) v. Canada (Information Commissioner)* appears to me to be consistent with the opinions of the dissenting justices on the issue of irreparable harm. Thus, the applicant has not proven irreparable harm.

[157] In *Longshore*, the Court of Appeal noted at para 26:

> The Unions allege unreasonable privacy invasion. This Court has made it clear that such bald allegations of unconstitutionality (including claims of privacy violations rooted in section 8 of the *Charter*) are not sufficient to establish irreparable harm under the tripartite *RJR-MacDonald* test (*Groupe Archambault Inc. v. CMRRA/SOCRAC Inc.*, 2005 FCA 330 at para. 16).

[158] The Federal Court of Appeal has also more recently highlighted the importance of establishing irreparable harm, in other contexts.

[159] In *Glooscap*, the Court of Appeal set a high standard for evidence of irreparable harm:

> [31] To establish irreparable harm, there must be evidence at a convincing level of particularity that demonstrates a real probability that unavoidable irreparable harm will result unless a stay is granted. Assumptions, speculations, hypotheticals and arguable assertions, unsupported by evidence, carry no weight. See *Dywidag Systems International, Canada, Ltd. v. Garford Pty Ltd.*, 2010 FCA 232 at paragraph 14; *Stoney First Nation v. Shotclose*, 2011 FCA 232 at paragraph 48; *Canada (Attorney General) v. Canada (Information Commissioner)*, 2001 FCA 25, 268 N.R. 328 at paragraph 12; *Laperrière v. D. & A. MacLeod Company Ltd.*, 2010 FCA 84 at paragraph 17.
>
> [32] The reason behind this was explained in Stoney First Nation as follows (paragraph 48):

> It is all too easy for those seeking a stay in a case like this to enumerate problems, call them serious, and then, when describing the harm that might result, to use broad, expressive terms that essentially just assert – not demonstrate to the Court's satisfaction – that the harm is irreparable.

[160] In *Gateway*, the Court of Appeal confirmed, at para 15, that"[g]eneral assertions cannot establish irreparable harm. They essentially prove nothing …" and reiterated the rationale set out in *Glooscap*.

[161] The jurisprudence from the Court of Appeal is, therefore, consistent in establishing that irreparable harm must be established with clear evidence, not hypothetical and speculative allegations. Allegations of a breach of section 8, without more, will not establish irreparable harm for the purpose of the tripartite test.

[162] In the present case, the applicants' allegations are based on the argument that privacy once lost cannot be regained and this is irreparable harm. This argument rests on the premise that the "search" or the provision of information in accordance with the screening measures is unreasonable. However, the applicants have offered no evidence of the irreparable harm that will be suffered by one or more of its members.

[163] In *Information Commissioner*, the Federal Court (*Canada (Attorney General) v Canada (Information Commissioner)*, [2000] FCJ No 1648 (QL), 187 FTR 1) had found that irreparable harm may result if safeguards for protecting the information were not followed or were not effective. However, the Court of Appeal noted at para 19 that no evidence was presented to show

that the provisions at issue were susceptible to breach or that any information had been improperly released by the Commissioner. The Court of Appeal also rejected the argument that the fact that the information would be reviewed by someone gave rise to irreparable harm:

> [21] There is no merit to this argument. Obviously, information must be reviewed by someone to give effect to the scheme set up by Parliament in implementing the Act. It cannot be seriously argued for instance that irreparable harm results when an authorized officer reviews information with the view of ensuring that personal information and other exempt information is protected from disclosure.

[164] The applicants' argument that merely providing information is a breach of their privacy resulting in irreparable harm similarly ignores the safeguards in place to protect the information and to ensure that it is not disclosed to anyone, other than those who are trained with respect to the handling and protection of the information and have a need to know, which would usually be only the Departmental Security Officer. The Standard describes the measures in place and the affidavit of Ms Whittle indicates that additional guidelines are under development. The respondent also noted the redress and review mechanisms with respect to any concerns that may arise regarding the screening measures. In addition, the information required to be provided is already in the hands or records of others (for example, credit reporting agencies have the credit information, RCMP records include criminal records, applications for employment include some biographical information, and various social media organizations store public information, some or all of which an employee may have publicly posted themselves). The provision of this same information to a Security Officer, who uses this information only to conduct a security assessment and does not share it further, cannot be assumed to constitute irreparable harm. No evidence has been provided to establish that it would.

[165] The applicants noted a particular concern about fingerprinting and assert that providing fingerprints at a police station, rather than in the workplace, will exacerbate the aura of criminality. As the respondent noted and as explained in the affidavit of Chief Superintendent Heffernan, fingerprinting is not part of the Standard *per se*. The Standard calls for a criminal records check. The RCMP has implemented fingerprinting as the state of the art method to conduct the criminal records check. Fingerprinting was also possible under the 1994 Standard. The applicants have not provided any evidence of how attending a police service to provide fingerprints will cause irreparable harm, particularly given that there are other non-criminal purposes for providing fingerprints. Moreover, the RCMP policy is not at issue in the underlying judicial review, nor in this motion.

[166] The Court will not assume that the applicants' allegations of infringement of section 8 of the *Charter*, of a breach of the *Privacy Act* or of abuse of discretion will succeed and that, therefore, the applicants have established irreparable harm.

[167] This would let the applicants "off the hook" for providing evidence of actual harm to an actual person pending the determination of the judicial review. In my view, this is not what the Supreme Court of Canada intended in confirming the three-part test and providing the guidance for each aspect of that test in *RJR-MacDonald*. If an applicant only needs to allege a *Charter* violation, which would meet the threshold for establishing a serious issue, and argue that irreparable harm is a foregone conclusion if the *Charter* violation is found, then the three-part test becomes a two-part test. This would ignore the balancing exercise and the factors to be considered before any determination is made as to whether the expectation of privacy is

reasonable and whether the search is reasonable. It would also ignore the safeguards in place to minimize any breach of privacy.

[168] In addition, the applicants' approach is contrary to the clear guidance of the Federal Court of Appeal that clear evidence of irreparable harm must be provided.

[169] Although the applicants have not merely asserted a *Charter* breach and have advanced arguments with reference to the jurisprudence with respect to the importance of protecting informational privacy against unreasonable search, and their allegations of serious issues cannot be characterized as "bald", their allegations of irreparable harm are simply "bald" allegations based on speculation.

[170] The applicants advised that they had no records to indicate how many and which of their members require only Reliability status. The applicants suggest that only 10% would require a higher security status or clearance. In a union of professionals covering a range of professional designations and across many departments and agencies, that estimate appears very low. I would expect a more significant percentage of the members to be required to hold a higher security level. Regardless, there is no evidence from any member(s) indicating that they will be screened for Reliability status and will suffer irreparable harm or will be required to disclose a change in their personal status and will suffer irreparable harm as a result between now and the time the judicial review is finally determined.

[171] While the Court acknowledges that one or some of the 35,000 members of the union would likely require that their security screening level be renewed between now and the determination of the judicial review and that all members are now subject to the requirement to report significant changes in their circumstances, for example, a criminal conviction, this does not establish that irreparable harm will be suffered by those persons. The Court should not be asked to make assumptions when the onus is on the applicants to provide some evidence to establish irreparable harm. The applicants have not provided an affidavit from Mr Aubry setting out his position and the level of security status or clearance he is required to have. Nor do we know when his security status will be renewed and whether he would be required to report any changes in his personal status or other circumstances, let alone how that would constitute irreparable harm to him pending the determination of the application for judicial review.

[172] The applicants' suggestion that they can bring a subsequent motion with concrete evidence of irreparable harm strikes me as an ultimatum to accept the applicants allegations of harm without any evidence to spare the Court a subsequent motion. Moreover, this approach ignores the onus on the applicants to provide non-speculative evidence of irreparable harm for this motion in accordance with the three-part test and the jurisprudence which highlights the requirement to establish irreparable harm.

Where does the Balance of Convenience lie?

The Applicants' Position

[173] The applicants submit that the balance of convenience favours preserving the *status quo*, which the applicants submit is the 1994 Standard. The applicants argue that Treasury Board has not demonstrated that the 1994 Standard, in place for over twenty years, is inadequate or that irreparable harm will result if the implementation of the Standard is delayed.

[174] Alternatively, the applicants take the position that if the *status quo* is found to be the 2014 Standard, then only the screening measures already implemented are part of that *status quo*.

[175] The applicants rely on two recent decisions which granted interim relief in the context of a union's challenge to security screening procedures: *Assn of Management, Administrative and Professional Crown Employees of Ontario v Ontario (Ministry of Government Services)*, [2009] OGSBA No 44, 181 LAC (4th) 385 [*Crown Employees*], where security clearance measures, including credit checks, for employees responsible for processing enhanced driver's licences, were stayed pending the determination of the policy grievance, and *Canada Post Corp v Canadian Union of Postal Workers (National Policy Grievance N00-12-00003, Arb Swan)*, [2013] CLAD No 256 [*Canada Post*], where new security screening measures, including criminal records checks, were stayed for twenty days.

[176] The applicants acknowledge the growth of threats related to intelligence and security due to terrorism and extremism, but argue that this is not a relevant consideration for public servants who hold only Reliability status.

[177] The applicants also argue that the rationale of requiring a Standard in order to maintain the confidence of Canada's allies does not apply to public servants holding Reliability status, who are not involved in positions relating to intelligence or security and do not have access to secret or top secret information. Similarly, the applicants dispute that Canadians would lose trust in public servants holding Reliability status who have not been subject to the screening measures at issue.

[178] The applicants submit that the growth of the internet since the previous Standard was implemented is not a compelling justification for the new screening measures. If it were, changes to the 1994 Standard should have been made long before 2014.

[179] The applicants dispute that there will be a policy vacuum if the screening measures at issue in the 2014 Standard for those requiring Reliability status are enjoined. The applicants submit that the 1994 Standard could be reinstated. Alternatively, those requiring a higher level of security status could be exempted from the stay or there could be a combination of the 1994 Standard for those requiring Reliability status and the 2014 Standard for those requiring other levels of screening.

[180] The applicants' position is that the harm that will be suffered by them if the Standard is implemented exceeds the harm to the respondent if the injunction is granted and its implementation is halted pending the determination of the application for judicial review.

The Respondent's Position

[181] The respondent points out that the relevant factors to consider in assessing the balance of convenience are the nature of the relief sought, the harm the parties allege, the nature of the legislative scheme under attack and the public interest (*RJR-MacDonald* at 350).

[182] The purpose of an interlocutory injunction is generally to maintain the *status quo*. The status quo to be considered when assessing the balance of convenience is the *status quo* at the time the application is made or heard (*China Ceramic Proppant Ltd v Carbo Ceramics In*c, 2004 FCA 283 at para 7, 34 CPR (4th) 431). At the time of this application and presently, the *status quo* is that the 2014 Standard is in place and implementation has commenced. An injunction would change the *status quo* by disrupting the implementation of the 2014 Standard.

[183] The respondent further submits that the promotion of the public interest is an important factor in assessing the balance of convenience. The promotion of the public interest is assumed in cases involving a challenge to a law, regulation or activity with a public interest purpose (*RJR-MacDonald* at 348-349). Once established, the burden shifts to the applicants to establish that the suspension of the law or, in this case, the 2014 Standard, would be in the public interest.

[184] The respondent submits that the same principle applies to a government policy adopted in the public interest (*Canada (Citizenship and Immigration) v Ishaq*, 2015 FCA 90 at paras 11-15 [*Ishaq*]).

[185] The Court must, therefore, assume that the policy was undertaken in the public interest. Once established, the onus shifts to the applicants to establish that suspension of the Standard, pending the determination of the judicial review, is in the public interest.

[186] In *Longshore*, the Federal Court of Appeal held that the public interest purpose of security screening regulations adopted to protect the public and the economy from terrorism and organized crime was undeniable (at para 46). The Court of Appeal noted in *Marine Transportation Reference*, in the context of assessing a breach of section 8, that courts should be prepared to allow the government a margin of appreciation where national security is at issue (at para 53). The respondent submits that the same reasoning applies in the present case. In addition, the public interest in national security underlying the Standard is clear from the text of the Standard.

[187] There is also a public interest in maintaining international relations and in maintaining the trust and confidence of Canadians in the government employees who administer and deliver programs and services and have access to a wide range of information from and about citizens. The public has an interest in ensuring that government employees who handle their information are properly screened.

[188] The respondent submits that irreparable harm would result from the granting of the injunction. It would create a policy vacuum, given that the 1994 Standard has been rescinded. It would create a serious gap in Canada's security screening capabilities and undermine Canada's relationships with its allies and their confidence in Canada's security scheme. It would leave Canada without measures to respond to the modern technological environment. In addition, the suspension of the 2014 Standard would lead to confusion about which security screening measures can or must be conducted and with respect to which employees, which increases the risk of adverse information not being uncovered, and poses a risk to Canada's interests.

[189] The respondent adds that the applicants' recent narrowing of its motion to specific screening measures for employees requiring Reliability status is not feasible and is impractical. The screening measures for Reliability status are the foundation for all security clearances and Enhanced screening.

[190] The respondent submits that the balance of convenience favours the respondent and the Treasury Board should continue the implementation of the Standard.

The Balance of Convenience Favours the Respondent

[191] The Supreme Court of Canada explained the third part of the test, the balance of inconvenience (or convenience), in *RJR-MacDonald* at 348-349, as follows:

> The third branch of the test, requiring an assessment of the balance of inconvenience to the parties, will normally determine the result in applications involving Charter rights. A consideration of the public interest must be taken into account in assessing the inconvenience which it is alleged will be suffered by both parties.

> These public interest considerations will carry less weight in exemption cases than in suspension cases. When the nature and declared purpose of legislation is to promote the public interest, a motions court should not be concerned whether the legislation has in fact this effect. It must be assumed to do so. In order to overcome the assumed benefit to the public interest arising from the continued application of the legislation, the applicant who relies on the public interest must demonstrate that the suspension of the legislation would itself provide a public benefit.
>
> [Emphasis added]

[192] The Court also noted that many factors must be considered in assessing the balance of inconvenience and these will vary in each case (at 342-343). In addition, public interest is a key consideration in cases involving *Charter* claims and will carry more weight where the application seeks to suspend an order or policy rather than exempt someone from its application (at 343, 346-347).

[193] In *Harper*, the Supreme Court of Canada, in the context of an application to stay the enforcement of election spending limits, noted the competing considerations in assessing the balance of convenience at para 5:

> Applications for interlocutory injunctions against enforcement of still-valid legislation under constitutional attack raise special considerations when it comes to determining the balance of convenience. On the one hand stands the benefit flowing from the law. On the other stand the rights that the law is alleged to infringe. An interlocutory injunction may have the effect of depriving the public of the benefit of a statute which has been duly enacted and which may in the end be held valid, and of granting effective victory to the applicant before the case has been judicially decided. Conversely, denying or staying the injunction may deprive plaintiffs of constitutional rights simply because the courts cannot move quickly enough: R. J. Sharpe, *Injunctions and Specific Performance* (loose-leaf ed.), at para. 3.1220.

[194] The Court also cited the test in *RJR-MacDonald* and noted that a validly enacted law is presumed to be in the public interest at para 9:

> Another principle set out in the cases is that in considering the grant of an interlocutory injunction suspending the operation of a validly enacted but challenged law, it is wrong to insist on proof that the law will produce a public good. Rather, at this stage of the proceeding, this is presumed. As Sopinka and Cory JJ. stated in *RJR--MacDonald Inc. v. Canada (Attorney General)*, [1994] 1 S.C.R. 311, at pp. 348-49:
>
> > When the nature and declared purpose of legislation is to promote the public interest, a motions court should not be concerned whether the legislation actually has such an effect. It must be assumed to do so. In order to overcome the assumed benefit to the public interest arising from the continued application of the legislation, the applicant who relies on the public interest must demonstrate that the suspension of the legislation would itself provide a public benefit.
>
> It follows that in assessing the balance of convenience, the motions judge must proceed on the assumption that the law -- in this case the spending limits imposed by s. 350 of the Act -- is directed to the public good and serves a valid public purpose. This applies to violations of the s. 2 (b) right of freedom of expression; indeed, the violation at issue in RJR--MacDonald was of s. 2 (b). <u>The assumption of the public interest in enforcing the law weighs heavily in the balance. Courts will not lightly order that laws that Parliament or a legislature has duly enacted for the public good are inoperable in advance of complete constitutional review, which is always a complex and difficult matter. It follows that only in clear cases will interlocutory injunctions against the enforcement of a law on grounds of alleged unconstitutionality succeed</u>.
>
> [Emphasis added]

[195] In *Ishaq*, the Federal Court of Appeal found that the principles set out in *RJR-MacDonald* with respect to irreparable harm to the public interest apply to policies as well as statutes and regulations if the policy is adopted to promote or protect the public interest (at paras 11-13).

[196] At para 15, the Court of Appeal held:

> In my view, there is no basis to depart from the general rule that irreparable harm to the public interest will arise if a policy undertaken for the promotion or protection of the public interest has been impugned. Based on the comments of the Supreme Court in paragraph 71 of RJR-MacDonald, this general rule will apply if there is "some indication" that the Policy in question was adopted by CIC pursuant to its responsibility for promoting or protecting the public interest in relation to admitting individuals as citizens.

[197] In summary, with respect to the assessment of the balance of convenience where *Charter* claims are made, the jurisprudence has established the following:

- Such applications for interlocutory injunctions raise special considerations and the competing interests must be considered; for example, an interlocutory injunction may deprive the public of the benefit of a policy or legislation which may ultimately be found to be valid, whereas denying the injunction may deprive applicants of constitutional rights simply because the courts cannot move quickly enough (*Harper* at para 5).
- The public interest is a key consideration in cases involving *Charter* claims and will carry more weight where the application seeks to suspend the policy or legislation at issue rather than exempt a person from its application. (*RJR-MacDonald* at 343, 346-347).
- When the nature and declared purpose of legislation is to promote the public interest, the Court should not be concerned whether the legislation has in fact this effect; it must be assumed to do so (*RJR-MacDonald* at 348-349).
- The Court should not insist on proof that the law will produce a public good (*Harper* at para 9).

- Only in clear cases will interlocutory injunctions against the enforcement of a law on grounds of alleged unconstitutionality succeed (*Harper* at para 9).
- In order to overcome the assumed benefit to the public interest arising from the continued application of the legislation, the applicant who relies on the public interest must demonstrate that the suspension of the legislation would in fact provide a public benefit (*RJR-MacDonald* at 348-349).
- The assumption regarding legislation enacted in the public interest also applies to a policy adopted to promote and protect the public interest (*Ishaq* at paras 11-15).

[198] In the present case, the applicants argue, among other issues, that their *Charter* protected privacy rights will be violated by the screening measures of the Standard and seek a suspension of the implementation of these measures pending the disposition of the judicial review. The public interest must, therefore, be considered and given considerable weight.

[199] Clearly, the government has the responsibility and authority to make policy regarding the security screening of its employees and contractors. Treasury Board wears two hats: as the employer and as the government department responsible for ensuring that policies are developed and implemented to ensure the proper administration of the government, including security policies for employees and contractors.

[200] The respondent has highlighted the government's motivation for the Standard, including the domestic and international threat environment, the physical and operational environment of

the government, and that the previous standard was outdated compared to the standards of Canada's allies. The affidavit of Ms Whittle explained the rationale for the 2014 Standard, which includes the need to respond to the evolving nature of threats to the security of Canada, to protect the vast amounts of information now accessible in interconnected information systems and, more generally, to respond to today's working environment. That evidence is uncontradicted and provides more than "some" indication that the Standard was adopted in the public interest. The Court is, therefore, not required to determine whether the Standard already has the effect it purports to have (*RJR-MacDonald* at 348-349).

[201] Although the applicants downplay the impact of changes to government technology and interconnectivity to security screening, government employees now have access to government systems and information that were not contemplated in 1994 or 2002 and the technology is evolving rapidly.

[202] The balance of convenience requires an assessment of the relative harm to both parties. In weighing and comparing the harm to the applicants and harm to the respondent, the respondent has provided evidence about the public interest addressed by the Standard. In addition, the respondent benefits from the assumption that the policy was developed and adopted in the public interest. The applicants have not provided any evidence that the public interest would be harmed by the implementation of the Standard pending the determination of the judicial review. The applicants only assert that the rationale advanced by the respondent for the Standard, including that it will protect the public interest, increases trust of Canadians and complies with

commitments made to international partners, is not sufficient to justify the Standard. This falls well short of rebutting the assumption and establishing any harm to the public interest.

[203] The respondent's characterization of the *status quo* is correct; the 2014 Standard has been adopted and implementation activities have begun and will continue over 36 months. The balance of convenience favours retaining the *status quo*.

[204] The applicants relied on *Crown Employees* and *Canada Post* to support their argument that an injunction should be granted despite the implementation of the screening measures. However, in both cases, which were decided in the context of policy grievances, the arbitration board did not apply all aspects of the *RJR-MacDonald* test and the application for the injunction was brought before the new measures were instituted. In *Canada Post*, the application was brought at the very last minute – but it was before the implementation of the security measures – and the Board suspended implementation for twenty days pending determination of the policy grievance.

[205] As the respondent points out, Reliability status is the foundation for all security clearances and Enhanced screening. Therefore, the applicants' suggestion that the screening measures should not be implemented with respect to employees requiring only Reliability status would be impractical, if not impossible, ineffective and would thwart the intended benefits of the new screening measures, which are presumed to be in the interest of the public. To apply different screening measures for employees requiring Reliability status – for example, only the measures in the 1994 Standard – would require a reinstatement of the 1994 Standard for

particular positions or individuals, with other employees being screened in accordance with the new measures. In my view, this would be impractical, inefficient and costly, and would create inconsistency, confusion and gaps in security screening pending the determination of the judicial review.

[206] Moreover, many of the same measures now required in the 2014 Standard could have been required on an optional basis pursuant to the 1994 Standard; for example fingerprints could have been required where a name-based criminal records check was inconclusive, disclosure of outstanding criminal charges could have been provided on a case-by-case basis, and open source inquiries were not prohibited and likely occurred without any parameters for the use of the information. In addition, credit checks could have been conducted in particular circumstances and for particular positions. As a result, enjoining the new measures, if the test for an injunction had been met, may have very little practical impact.

[207] Modernization of the Standard is in the public interest. The advances of technology cannot be ignored. On the one hand, technology that allows broad access to networks of information and collaborative work environments has many benefits, but, on the other hand, permits a wider range of people to access information they otherwise had no access to and no need to access. With this comes the need to ensure that all employees who work in such environments are security screened and informed of their obligations with respect to their access to this information. Establishing where the line should be drawn between protecting the privacy of government employees and ensuring government programs operate in a secure environment is not the role of the Court on this motion.

[208] The judicial review will grapple with the issue of whether and how an employee's reasonable expectation of privacy in terms of sharing personal information has evolved due to the current environment, what is objectively reasonable and whether the provision of information in this context is reasonable.

[209] Pending the determination of the application for judicial review, the Court will not enjoin the implementation of the 2014 Standard. The applicants have raised one or more serious issues, but have not established with any non-speculative evidence that any one of its members will suffer irreparable harm in the interim period. Moreover, the balance of convenience favours the respondent's continued implementation of a policy adopted in the public interest.

[210] Again, I note the words of the Supreme Court of Canada in *Harper* at para 9:

> […] The assumption of the public interest in enforcing the law weighs heavily in the balance. Courts will not lightly order that laws that Parliament or a legislature has duly enacted for the public good are inoperable in advance of complete constitutional review, which is always a complex and difficult matter. It follows that only in clear cases will interlocutory injunctions against the enforcement of a law on grounds of alleged unconstitutionality succeed.

[211] This is not one of those clear cases.

ORDER

THIS COURT ORDERS that the motion for an interlocutory injunction is dismissed.

No costs are ordered.

"Catherine M. Kane"
Judge

FEDERAL COURT

SOLICITORS OF RECORD

DOCKET:	T-551-15
STYLE OF CAUSE:	THE PROFESSIONAL INSTITUTE OF THE, PUBLIC SERVICE OF CANADA AND STÉPHANE AUBRY v ATTORNEY GENERAL OF CANADA
PLACE OF HEARING:	OTTAWA, ONTARIO
DATE OF HEARING:	JULY 8, 2015
ORDER AND REASONS:	KANE J.
DATED:	SEPTEMBER 22, 2015

APPEARANCES:

Mr. Steven Welchner Ms Isabelle Roy	FOR THE APPLICANTS
Ms. Anne Turley Mr. Youri Tessier-Stall	FOR THE RESPONDENT

SOLICITORS OF RECORD:

Welchner Law Office Professional Corporation Ottawa, Ontario	FOR THE APPLICANTS
William F. Pentney Deputy Attorney General of Canada Ottawa, Ontario	FOR THE RESPONDENT