

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation: *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner)*,
2012 BCSC 875

Date: 20120614
Docket: 11-0108
Registry: Victoria

**In the Matter of the *Judicial Review Procedure Act*,
R.S.B.C. 1996, c. 241**

and

**In the Matter of the Decision of the Information and Privacy Commissioner
of British Columbia (Order No. F10-39), dated November 25, 2010,
made under the Freedom of Information and Protection of
Privacy Act, R.S.B.C. 1996, c. 165**

Between:

Minister of Citizens' Services

Petitioner

And:

**Information and Privacy Commissioner of British Columbia
IBM Canada Limited, and
BC Freedom of Information and Privacy Association**

Respondents

Before: The Honourable Mr. Justice Bracken

Reasons for Judgment

Counsel for the Petitioner:

J. M. Walters and J. M. Tuck

Counsel for the Respondent
Information and Privacy Commissioner
of British Columbia:

D. K. Lovett, Q.C.

Counsel for the Respondent
BC Freedom of Information and
Privacy Association:

S. Hern

Place and Date of Trial/Hearing:

Victoria, B.C.
March 8 and 9, 2012

Place and Date of Judgment:

Victoria, B.C.
June 14, 2012

[1] The Ministry of Citizens' Services (the "Ministry") seeks judicial review of a decision by a delegate of the Information and Privacy Commissioner of British Columbia (the "Adjudicator") pursuant to the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c.165 (the "Act") relating to an access request made by the British Columbia Freedom of Information and Privacy Association ("FIPA").

Background

[2] These background facts are largely drawn from the summary of facts contained in the respondent's Reply to Petition. It does not appear these facts are disputed in any material way.

[3] On December 9, 2004, FIPA sought access to a Workplace Support Agreement dated December 3, 2004 between the Province of British Columbia and IBM Canada Ltd. (the "Agreement"). The Agreement governs IBM's provision of computer support services to the Ministry and is part of a larger Master Services Agreement between the parties.

[4] The Agreement was reached following a "Core Review" of the way in which government services are delivered in an effort to establish a more efficient way of delivering government services to British Columbians and to improve its information technology and information management. The agreement is one of nine Alternative Service Delivery contracts entered into by the Province using a process known as the Joint Solutions Procurement process. The process requires the government to

share an unprecedented amount of sensitive material with the private sector vendor of the service.

[5] The Agreement requires IBM staff to provide service desk functions to government employees who require assistance in relation to the use and performance of their workplace systems.

[6] FIPA requested that the Ministry disclose the following: a list of software IBM uses to manage the Province's computer system; server names and the locations of those servers; and a list of certain IBM equipment used by IBM to carry out its obligations under the Agreement.

[7] On January 11, 2010, the Ministry released information responding to FIPA's initial request. However, the Ministry withheld portions of the requested information pursuant to ss. 15, 17, 21 and 22 of the *Act*.

[8] FIPA sought review of the Ministry's decision to withhold information pursuant to ss. 15, 17, and 21 but accepted the Ministry's decision to withhold information pursuant to s. 22 of the *Act*.

[9] On review, the Adjudicator concluded that the Ministry was required to disclose the information that had been withheld under ss. 15 and 17 of the *Act*.

[10] The Ministry now seeks to have the Adjudicator's order pursuant to s. 15(1)(l) of the *Act* reviewed by this Court.

[11] Section 15(1)(l) of the *Act* reads as follows:

15(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to ...

(l) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

Standard of Review

[12] Both parties agree that the appropriate standard of review is reasonableness. The Supreme Court of Canada in *New Brunswick (Board of Management) v.*

Dunsmuir, 2008 SCC 9, defined the reasonableness standard and explained how it should be applied to administrative decisions. The majority held the following at para. 47:

Reasonableness is a deferential standard animated by the principle that underlies the development of the two previous standards of reasonableness: certain questions that come before administrative tribunals do not lend themselves to one specific, particular result. Instead, they may give rise to a number of possible, reasonable conclusions. Tribunals have a margin of appreciation within the range of acceptable and rational solutions. A court conducting a review for reasonableness inquires into the qualities that make a decision reasonable, referring both to the process of articulating the reasons and to outcomes. In judicial review, reasonableness is concerned mostly with the existence of justification, transparency and intelligibility within the decision-making process. But it is also concerned with whether the decision falls within a range of possible, acceptable outcomes which are defensible in respect of the facts and law.

[13] In reaching my conclusion I acknowledge that the Adjudicator's interpretation of his home statute, based on his expertise and polycentric functions, is to be afforded deference. *Pushpanathan v. Canada (Minister of Citizenship and Immigration)*, [1998] 1 S.C.R. 982, at para. 36, *Pezim v. British Columbia (Superintendent of Brokers)*, [1994] 2 S.C.R. 557, *Dunsmuir v. New Brunswick*, 2008 SCC 9, *Canada (Citizenship and Immigration) v. Khosa*, 2009 SCC 12, and *British Columbia Teachers' Federation v. British Columbia (Information and Privacy Commissioner)*, 2006 BCSC 131.

[14] Before turning to the substantive elements of this review, I wish to address at the outset the admissibility of Ms. Christine Fairey's affidavit as evidence on this judicial review.

Admissibility of the Affidavit of Christine Fairey

[15] A significant issue in this case is the Ministry's submission that the delegate failed to consider relevant factors. In particular, that the delegate failed to take into consideration the *International Standard, ISO/IEC 17799 (2nd Edition) - Information technology - Security techniques - Code of practice for information security management, and Technical Corrigendum 1*, published 2007-07-01 and the

Guidelines for Audits of Automated Personal Information Systems, OIPC Guideline 01-01, dated October 10, 2001.

[16] The Ministry argues these guidelines have been referred to by the Commissioner in past decisions and that they create a specialized system of standards for information security and the Adjudicator should have taken “official notice” of them. (See, for example: Investigation Report 11-01, paras. 56-57). However, there was apparently no reference to the guidelines before the Adjudicator and I agree with counsel for the Commissioner that just because the guidelines exist and may have been referred to in the body of the contract does not make them part of the record of proceeding.

[17] In *Waters v. British Columbia, (Director of Employment Standards)*, 2004 BCSC 1570, Romilly J. similarly explained:

[25] ... It is not a question of whether the Court would reach the same conclusion on the evidence, but rather whether there is any evidence to support the conclusion of the decision maker. In assessing this evidence it is also important to note that judicial review is concerned with assessing the evidence that was before the tribunal and not additional evidence that is tendered after the fact.

[18] In *Telus Communications Co. v. Telecommunications Workers Union*, 2009 BCSC 1289, Pearlman J. confirmed the following legal principles regarding the admissibility of evidence on a judicial review:

[29] Evidence extrinsic to the record may be admissible to show lack of jurisdiction or denial of natural justice: *Evans Forest Products Ltd. v. British Columbia (Chief Forester)*, [1995] B.C.J. No. 729 (B.C.S.C.) at para. 4.

[30] In *Karbalaeiali v. British Columbia (Deputy Solicitor General)*, 2006 BCSC 13 the court stated at paras. 53 and 54 that the rule against admitting fresh evidence on a judicial review is not absolute, but emphasized that only extrinsic evidence relevant to the issues of lack of jurisdiction or denial of natural justice may be admitted.

[19] More recently in British Columbia the issue of whether a party in a judicial review proceeding can present evidence that was not part of the official “record” of the proceedings arose in *SELI Canada Inc. v. Construction and Specialized Workers' Union, Local 1611*, 2011 BCCA 353. During the course of that hearing

there was no official reporter. A secretary for legal counsel for the employer had recorded the proceedings and prepared a transcript.

[20] At the hearing of the judicial review in *SELI*, the chambers judge held:

[77] On a judicial review it is not the court's role to re-evaluate or re-weigh the evidence and the court must maintain an attitude of deference to a tribunal's fact-finding role. The court is however mandated by s. 59 of the *ATA* to scrutinize the evidence to determine whether there is evidence to support findings of fact and whether such findings are reasonable in light of all the evidence. The court cannot carry out its statutory mandate if the evidence is not before it.

[21] On appeal, Groberman J.A. held that the transcripts were not part of the record saying at para. 51:

[51] In my view, the documents in question on this appeal do not fall within the traditional concept of the record. They are not documents which were before the tribunal, nor are they documents which emanated from it. If the only basis for judicial review in this case were "error of law on the face of the record", then, I would find that the documents are not admissible.

[22] Later, at paras. 68 - 69, the following was stated:

[68] In *142445 Ontario Limited, c.o.b. as Utilities Kingston v. International Brotherhood of Electrical Workers, Local 636* (2009), 251 O.A.C. 62, 95 Admin L.R. (4th) 273, Ontario's Divisional Court revisited the question of the admissibility of affidavits to establish what evidence was before a tribunal. The court found that such affidavits should not generally be admitted. At paras. 32-33, the court said:

[32] If extensive affidavits can be filed on applications for judicial review in order to permit parties to challenge findings of fact before such tribunals, there would be a significant incentive for parties to seek judicial review since they could then attempt to reframe the evidence that was before the arbitrator. As a result, the process of judicial review is likely to be more prolonged and more costly. ...

[69] ... It is true that extensive affidavits or transcripts will assist a party who sets out to abuse the process of the court by trying to turn a judicial review application into a hearing *de novo*. A court need not tolerate such a practice, and can refuse to admit affidavit evidence if it is not relevant to a genuine ground of judicial review. The fear of abuse should not be a basis for refusing to admit affidavit evidence where it is filed in support of a recognized basis for judicial review.

[23] The aforementioned case law indicates that additional affidavit material will only be admitted when it directly relates to a ground of review (specifically pertaining

to a lack of jurisdiction or denial of natural justice) and when there is little or no risk of recreating the evidence before the tribunal.

[24] The Adjudicator has the right to determine the extent of its record, and this Court is not entitled to look beyond that record in undertaking a judicial review. Resort to extrinsic evidence, such as the Fairey affidavit, may only be made to show lack of jurisdiction or a denial of natural justice.

[25] The only case cited for the proposition that the Fairey affidavit is “not part of the record as that is generally considered” but rather comprises documents that the Commissioner ought to have taken official notice of is *British Columbia (Minister of Water, Land and Air Protection) v. British Columbia (Information and Privacy Commissioner)*, 2002 BCSC 1429 (“MWLA”).

[26] The context in which this statement was made is relevant: The province argued that it was not advised that the Commissioner had obtained a copy of a topographical map with UTM grids. It complained that it was procedurally unfair not to allow it to make submissions about the Commissioner's conclusions of accuracy of the information and the inferences he drew from reviewing this independent research.

[27] Madam Justice Satanove did not find any unfairness in the procedure used by the Commissioner. She held:

[24] ... MWLA raised the issue of the map and UTM co-ordinates in its submissions. It relied on the existence of such maps in the public domain in support of its argument that armed with the Information and one of these maps, individuals could locate live grizzly bears and cause them harm. The maps were described and discussed by MWLA witnesses but no copies were provided to the Commissioner. When he did obtain one of these maps, he found the representations of MWLA through its counsel to be without merit.

[25] MWLA does not challenge the Commissioner's jurisdiction to take official notice of the map and UTM co-ordinates, but submits that the Commissioners should have notified it as to what he intended to make of it, so they could persuade him otherwise.

[26] It is trite law that official notice may be taken by a decision maker on his or her own initiative. Furthermore, the generally accepted modern view is that where official notice is taken of a matter, the official notice is final. (*R. v.*

Zundel (1987), 35 D.L.R. (4th) 338 at 391 (Ont. C.A.), appeal allowed on other grounds, [1992] 2 S.C.R. 731). This is because facts which are capable of official notice are so generally known and accepted they cannot be reasonably challenged. Therefore the very nature of facts subject to official notice should not trigger the need for additional submissions, especially when they have been within the prior knowledge of the party complaining.

[27] In its submissions MWLA also objected to the Commissioner having viewed maps of the Alaska panhandle. Once again the subject of Alaska was raised by MWLA and the size of the area in question was an indisputable fact which should have been known to MWLA or its experts.

[28] In my opinion, the case of *MWLA* does not provide support for the petitioner's argument that the Commissioner ought to have taken official notice of the documents in question. It appears that para. 26 was taken out of context. It is also of note that this decision has not been cited in any Canadian court on the point of "official notice."

[29] The Adjudicator did not include the material located in the *Fairey* affidavit as part of the record. The issues raised on this review do not pertain to issues of natural justice or lack of jurisdiction. Therefore, this court cannot consider the material located in the *Fairey* affidavit.

[30] It is my view that to "admit" the *Fairey* affidavit would in effect turn this judicial review into a hearing *de novo*, and the affidavit is therefore not admissible upon this review.

Position of the Ministry on this Review

[31] The Ministry seeks the following relief:

1. An order quashing those portions of the Adjudicator's Order requiring the Ministry to provide the applicant access to the information the Ministry withheld under s.15(1)(l) of the *Act*.
2. A declaration that the Ministry is entitled to withhold the information from disclosure pursuant to s.15(1)(l) of *FOIPPA*.

3. In the alternative, or further, an order referring the question of whether the Ministry can withhold the requested information under s.15(1)(l) back to the Information and Privacy Commissioner with directions as to the appropriate test to be applied under s.15 or alternatively with directions as to appropriate factors to consider in articulating the test to be applied under s.15 in this context.

4. An order that a referral of the question back to the Information and Privacy Commissioner will be for a new hearing, and the parties are entitled to file further evidence or submissions, or both, as the parties consider necessary.

[32] The Ministry argues that the Adjudicator erred in applying a test that required the Ministry to provide evidence that disclosure would more likely than not result in a successful breach of the entire security system.

[33] More specifically, the Ministry argues that the Adjudicator erred in:

- a) Failing to properly interpret the terms “security of ... a computer system” and “harm” to that system pursuant to s.15(1)(l);
- b) Articulating the harm at stake by disclosing the information;
- c) Failing to consider the relevant context of the Ministry’s claim under s.15 including the Ministry’s obligations to provide reasonable security of personal information under s. 30 of *FOIPPA*, the nature of security of electronic data, the contractual obligations of the parties to the Agreement, the direction from the Information and Privacy Commissioner to use best practices for the security of electric personal information and the sensitive personal information protected by the computer system;
- d) Selecting the appropriate test and evidentiary requirements for the reasonable expectation of harm to the security of a computer system;
- e) Failing to provide adequate reasons;

- f) Reaching a decision that does not fall within a reasonable range of possible acceptable outcomes.

Position of the Respondent

[34] It is the respondent's position that the Adjudicator:

- a) understood and correctly articulated the test under s.15(1)(l);
- b) correctly assessed the evidence against that test; and
- c) provided reasons that are sufficiently clear, precise and intelligible.

[35] The respondent emphasizes that the Adjudicator's order is to be assessed against the deferential standard of reasonableness. Under the reasonableness standard tribunals have a margin of appreciation within a range of acceptable and rational solutions.

[36] The respondent further argues that this margin of appreciation is considerably wider when a decision formulates or implements broad public policy, as is the case here.

Analysis

Section 15(1)(l) Framework

[37] Although I am not to interpret the statutory provisions in question *de novo*, I note that s. 15 uses the permissive "may" rather than the imperative "shall." It is not a requirement that the Ministry refuse to disclose information to an applicant if the disclosure could reasonably be expected to harm the security of any property or system including a computer or communication system.

[38] Section 15 also provides that before a public body, such as the Ministry, is entitled to withhold information it must adduce sufficient evidence to demonstrate the disclosure of the information could reasonably be expected to harm the security of a computer system.

[39] Section 57 of the *Act* articulates that the burden of proof rests with the Ministry to establish its authority to withhold requested information under s.15(1)(l).

[40] Further, s.15 sets out as a criterion for withholding information that disclosure in and of itself creates a reasonable expectation of harm.

[41] Consequently, if the public body fails to meet the harms-based test, it is not entitled to withhold the requested information.

The Harms-based Test Pursuant to s.15(1)(l)

[42] The Adjudicator articulated the test under s. 15(1)(l) as follows:

[14] The identified harm at issue here is the unauthorized entry into the Province's computer system by hackers. Would it be reasonable to expect the release of the withheld information to lead to this harm?

[43] The Adjudicator's ruling clearly articulates that a) it is the release of the information itself which must give rise to a reasonable expectation of harm, and b) the burden rests with the Ministry to establish that the disclosure of the information in question could result in the identified harm.

[44] Accordingly, the Adjudicator correctly articulated the test pursuant to s.15(1)(l) of the *Act*.

[45] In assessing the evidence against the test, the Adjudicator held:

[7] In assessing the Ministry's application of s.15(1)(l), I have taken the same approach as previous Orders including Order 00-01. Commissioner Loukidelis outlined, in that Order, the nature of the evidence required to meet a harms-based test such as that set out s.15(1):

... a public body must adduce sufficient evidence to show that a specific harm is likelier than not to flow from disclosure of the requested information. There must be evidence of a connection between disclosure of the information and the anticipated harm. The connection must be rational or logical. The harm feared from disclosure must not be fanciful, imaginary or contrived.

[46] In outlining the nature of the evidence required to meet the harms-based test pursuant to s.15(1)(l), the Adjudicator adopted well-accepted evidentiary

requirements. See *Order F11-23; British Columbia Lottery Corp. (Re)*, [2011] B.C.I.P.C.D. No. 29 at para. 29; *Order F11-14; British Columbia (Ministry of Finance) (Re)*, [2011] B.C.I.P.C.D. No. 19 at para. 10; *Order F11-13; BC Coroners Service (Re)*, [2011] B.C.I.P.C.D. No. 18 at para. 8; *Order F10-25; British Columbia (Ministry of Health Services) (Re)*, [2010] B.C.I.P.C.D. No. 36 at para. 17; *Order 00-01; Langley (Township) (Re)*, [2000] B.C.I.P.C.D. No. 1, at para. 22.

The Adjudicator's Application of the s.15(1)(l) Framework

[47] In assessing the evidence against the s.15 harms-based test, the Adjudicator recited the following portion of the Ministry's argument at para. 11:

A hacker who wanted to attack the [Province's computer system] but did not have access to the Section 15 Information, would have to guess as to the types of applications, equipment and the locations and names of servers. However, if a hacker already had access to the Section 15 Information, in whole or in part, they would not have to guess or would, at the very least, not have to guess as much. This increases their chances of successfully compromising the security of the [s]ystems.

[48] FIPA's response to the Ministry's argument was canvassed by the Adjudicator at para. 12. It reads in part:

Criminals might try a door a number of times a year, but if the house had its street numbers removed and the marker of the locks filed off they would be less likely to succeed in gaining entry ... The information being withheld ... is the equivalent to street numbers and lock manufacturers, not the key to the door or the password for the alarm system.

[49] The Adjudicator ultimately agreed with FIPA and held as follows:

[15] I agree with the applicant that revealing the name of the system software does not provide a would-be criminal access to data in the Province's computer system. I would also add that knowing a server's location does not equate to gaining entry to it. The Ministry's submission that the information at stake is very sensitive strongly suggests that the Ministry's security system would be set up to prevent unauthorized access to any room or building that houses a server.

[16] Moreover, despite the Ministry's claims otherwise, it draws no direct connection between the disclosure of the disputed information and the claimed harm. Rather, the Ministry submits that the release of the information "increases" the "chances" of a successful attack. By what factor these chances are increased the Ministry does not explain. In effect, the

Ministry asks me to assume that the information disclosure could lead to a series of contingent events, the likelihood of which it leads me to guess, that might in turn lead to an unauthorized breach of the computer system. This proposition is clearly speculative. It certainly falls short of evidence required to show that the specific harm claimed is likelier than not to follow from the requested information's disclosure.

[17] I also note the Ministry's submissions impliedly acknowledge that, even without the disclosure of the requested information, a hacker could guess it. It stretches credibility to believe the Province's security system is so fragile that its breach is more likely than not based on a mere guess.

[50] In finding the Ministry's argument speculative and not persuasive, the Adjudicator demonstrated he was alive to recent jurisprudence in the area:

[18] My approach to this issue is consistent with Order F10-25, [[2010] B.C.I.P.C.D. No.36] ... [which] concerned records connected with another agreement reached under the ASD contract process. As here, the name of a computer server was among information withheld by the public body. The public body argued this disclosure would increase the vulnerability of the Province's computer system and data to attack. Senior Adjudicator Francis carefully considered the issues and stated:

I find the Ministry's arguments speculative and not persuasive. Disclosure of the information by itself, could not reasonably lead to the harm the Ministry fears. While the Ministry has provided general evidence regarding *modus operandi* of hackers, it has not provided any evidence of the risk that these techniques would be effective in relation to this particular server ... There must be something more that ties a special risk to a particular context so as to meet the "reasonable expectation" test. In this case, that test has not been met. ...

[51] Upon review of the aforementioned case law and the parties' submissions, the Adjudicator concluded "the Ministry has not met the burden of proving a reasonable expectation that the disclosure of the disputed information would result in the identified harm" (para. 19).

[52] The Adjudicator's reliance on case law analogous to the case at bar also demonstrates the Adjudicator's sensitivity to the context in which the Ministry's claim was made. Nothing in the reasons suggest that the Adjudicator viewed s.15 (1)(l) in isolation, as the Ministry suggests.

[53] Further, the Adjudicator, similar to a trial judge, is not required to refer to every item of evidence considered or to detail the way each item was assessed. As

noted by Binnie J. in *R v. Walker*, 2008 SCC 34, "Reasons are sufficient if they are responsive to the case's live issues and the parties' key arguments. Their sufficiency should be measured not in the abstract, but as they respond to the substance of what was in issue" (para. 20). This principle has been adopted in the administrative law context: *Magno (Re)*, [2008] B.C.E.S.T.D. No. 121; *New Vision Enterprises Ltd. (c.o.b. Quality Hotel) (Re)*., [2008] B.C.E.S.T.D. No. 122.

[54] However, the Ministry argues on the authority of *Merck Frosst Canada Ltd. v. Canada (Health)*, 2012 SCC 3, that while proof on a balance of probabilities is still required to meet the test of proof of future harm the evidence required will be affected by the nature of the proposition the applicant is seeking to establish.

[55] In that case the Court dealt with the federal *Access to Information Act*, R.S.C. 1985, c. A-1, which states:

20. (1) Subject to this section, the head of a government institution shall refuse to disclose any record requested under this Act that contains

...

(c) information the disclosure of which could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a third party; ...

[56] In discussing this case, it should be noted the provisions of s. 20 (1)(c) of the federal *Access to Information Act* are similar, but not identical to s. 15(1)(l) of our provincial *FOIPPA*. Secondly, the submission Merck made to the Supreme Court of Canada was that the Federal Court of Appeal had imposed a heavier burden than the civil standard of balance of probabilities. The Supreme Court of Canada agreed. Merck affirmed the civil standard at para. 94 where Cromwell J. for the majority said:

This notion of a "heavy burden" appears in many places in the jurisprudence relating to the exemptions: see, e.g., *AstraZeneca Canada Inc. v. Canada (Minister of Health)*, 2005 FC 189 (CanLII) (with supplementary reasons at 2005 FC 648 (CanLII)), at para. 52, aff'd 2006 FCA 241, 353 N.R. 84, and *Canada (Information Commissioner) v. Canada (Prime Minister)*, [1993] 1 F.C. 427 (T.D.) ("*Canada v. Canada*"), at p. 441. However, it is important to differentiate between the standard of proof and how readily that standard may be attained in a given case. It is now settled law that there is only one civil standard of proof at common law and that standard is proof on the balance of probabilities: *F.H. v. McDougall*, 2008 SCC 53, [2008] 3 S.C.R. 41, at

para. 40. Nothing in the Act suggests that we should depart from this standard. However, as noted in *McDougall*, "context is all important and a judge should not be unmindful, where appropriate, of inherent probabilities or improbabilities or the seriousness of the allegations or consequences" (para. 40). Proof of risk of future harm, for example, is often not easy. Rothstein J. (then of the Federal Court) captured this point in *Canada v. Canada* where he noted that there is a "heavy onus" on a party attempting to prove future harm while underlining that the obligation to do so requires proof on a balance of probabilities (p. 476). Therefore, I conclude that a third party must establish that the statutory exemption applies on the balance of probabilities. However, what evidence will be required to reach that standard will be affected by the nature of the proposition the third party seeks to establish and the particular context of the case.

[57] I am satisfied the Adjudicator applied the correct test and, as I have already noted, that he was clearly mindful of the context of this case and, in particular, the proposition of the Ministry that there was a risk of future harm if the information sought by FIPA was released.

[58] I am satisfied the Adjudicator's finding that the Ministry failed to establish a clear and direct connection between the disclosure of the withheld information and the alleged harm, falls within a range of possible, acceptable outcomes which are defensible in respect of the facts and law.

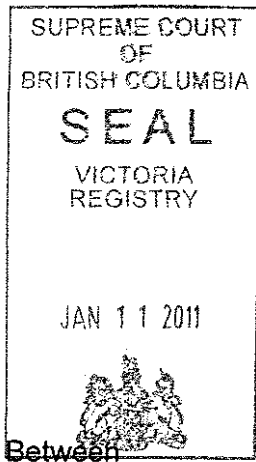
[59] There is an intelligible basis in the reasons for the decision. The Adjudicator informed the Ministry precisely what it lacked: concrete factors to demonstrate there was a reasonable expectation that sensitive government information would be "hacked" or otherwise compromised should the information in question be released.

[60] The Adjudicator articulated the chain of reasoning and the findings of fact on which the decision is based and his reasons do not merely recite facts and arguments put forth by the parties.

[61] I find that the Adjudicator acted reasonably by considering s.15(1) together on the facts and evidence before him. The reasons do not contain any misstatement of the law or other legal error.

[62] The Ministry's application is therefore dismissed.

"J. K. Bracken, J."
The Honourable Mr. Justice Bracken



Form 66 (Rules 16-1 (2) and 21-5 (14))

11 0108

No.

Victoria Registry

In the Supreme Court of British Columbia

Ministry of Citizens' Services

Petitioner

and

Information and Privacy Commissioner of British Columbia,
IBM Canada Limited, and
BC Information and Privacy Association

Respondents

PETITION TO THE COURT

This proceeding has been started by the petitioner(s) for the relief set out in Part 1 below.

If you intend to respond to this petition, you or your lawyer must

- (a) file a response to petition in Form 67 in the above-named registry of this court within the time for response to petition described below, and
- (b) serve on the petitioner(s)
 - (i) 2 copies of the filed response to petition, and
 - (ii) 2 copies of each filed affidavit on which you intend to rely at the hearing.

Orders, including orders granting the relief claimed, may be made against you, without any further notice to you, if you fail to file the response to petition within the time for response.

Time for response to petition

A response to petition must be filed and served on the petitioner(s),

- (a) if you reside anywhere within Canada, within 21 days after the date on which a copy of the filed petition was served on you,
- (b) if you reside in the United States of America, within 35 days after the date on which a copy of the filed petition was served on you,
- (c) if you reside elsewhere, within 49 days after the date on which a copy of the filed petition was served on you, or
- (d) if the time for response has been set by order of the court, within that time.

(1) The address of the registry is: 850 Burdett Avenue, Victoria, British Columbia

(2) The ADDRESS FOR SERVICE of the petitioner(s) is:

Ministry of Attorney General
Legal Services Branch
6th Floor – 1001 Douglas Street, Victoria, BC V8W 2C5

Fax number address for service (if any) of the petitioner(s): 250-356-9154

E-mail address for service (if any) of the petitioner(s):

(3) The name and office address of the petitioner's(s') lawyer is:

Jean Walters
Barrister and Solicitor
Ministry of Attorney General, Legal Services Branch, 6th Floor – 1001 Douglas Street,
Victoria, BC V8W 2C5
Telephone 250-356-8894

CLAIM OF THE PETITIONER

Part 1: ORDER(S) SOUGHT

1. An order in the nature of certiorari quashing those portions of Order No. F10-39 of the delegate of the Information and Privacy Commissioner, dated November 25, 2010, requiring the Ministry of Citizens' Services ("the Ministry") to provide the applicant in that case access to the information the Ministry withheld under section 15(1)(l) of the *Freedom of Information and Protection of Privacy Act* ("FOIPPA").
2. A declaration that the Ministry is entitled to withhold the information from disclosure pursuant to section 15(1)(l) of *FOIPPA*.
3. In the alternative, or further, an order referring the question of the entitlement of the Ministry to withhold the information from disclosure pursuant to section 15(1)(l) of *FOIPPA* back to the Information and Privacy Commissioner, with directions as to the appropriate test to be applied under s. 15, or alternatively, with directions as to appropriate factors to consider in articulating the test to be applied under s. 15 in the circumstances of this case.
4. An order that a referral of the question back to the Information and Privacy Commissioner will be for a new hearing, and the parties are entitled to file further evidence or submissions, or both, as the parties consider necessary.
5. Such other order as this Court considers just.

Part 2: FACTUAL BASIS

1. The Respondent, BC Freedom of Information and Privacy Association (FIPA), made a request to the Ministry under *FOIPPA* on or about December 9, 2004 for four alternative service delivery contracts, including the Workplace Support Agreement between the Province of British Columbia and the Respondent IBM Canada Ltd. ("the Agreement").
2. In 2001 the Government of British Columbia undertook a Core Review process in a desire to transform the way government services are delivered to British Columbians. Furthermore, it articulated a desire to explore Alternative Service Delivery (ASD) as a solution for resolving antiquated IT systems and inflexible, often manual business processes that could not adapt quickly to new policy and business needs.

The Agreement

3. The Agreement, worth \$300 million over 10 years, is one of nine ASD contracts have been entered into by the Province using the Joint Solutions Procurement (JSP) process.

4. The JSP process that British Columbia has developed is a unique approach to procurement that allows government and the private sector service providers to jointly develop a solution to meet the Province's unique needs. The JSP process requires vendors to share unprecedented amounts of highly sensitive information, of a nature not required in the past in more traditional procurement processes. In particular, the Province requires an extraordinary level of transparency between the parties so that the resulting contract is a complete record of the details of the arrangement and can be responsive to the situational changes that occur over the course of such long term contractual arrangements.
5. The Agreement is in the form of a written contract with 26 schedules ("A" to "Z").
6. The Agreement requires IBM staff to provide service desk functions and provide tools and processes to act as the single point of contact for government employees who require assistance in relation to the use and performance of their workplace systems, including the use of hardware and software.
7. Pursuant to the terms of the Agreement, IBM has access to, or custody of, various types of personal information contained on government computer systems. By law and under contract IBM is responsible for implementing various security arrangements for the protection and security of this information. Some of the types of information found on the computer systems that are the subject of security arrangements under the Agreement are:
 - Medical Services Plan information;
 - Child protection information;
 - Communicable disease information;
 - Income assistance information;
 - Criminal Justice information, including personal information in relation to victims and witnesses and criminal record information;
 - Pharmacare information;
 - Education information, including Kindergarten to Grade 12 and post secondary institutions;
 - Driver's licence information.
8. The information severed by the Ministry from the Agreement under section 15(1)(l) of FOIPPA fell into the following categories:
 - A list of software that IBM agrees to use in relation to managing the Systems and the version of the product in question (the "Software List"). This list is found in Schedule "I" of the Agreement;
 - Server names and the location of those servers. This list is found in Schedules "J" (pages J1 to J5, inclusive), "K", "L" (page L5) and "X" of the Agreement;

- Equipment List; Schedule "J" (pages J6 to J10, inclusive).

The Inquiry Process

9. The Ministry advised FIPA on or about February 17, 2005 that it had issued third party notice to the Respondent IBM Canada Ltd. (IBM) under s. 23 of FOIPPA with respect to the Agreement. Section 23(1) of the Act provides that if the head of a public body intends to give access to a record that the head has reason to believe contains information that might be excepted from disclosure under section 21 or 22, the head must give the third party a written notice under subsection (3).
10. On or about April 12, 2005 the Ministry advised FIPA under s. 24 of FOIPPA that following consultations with a third party (being IBM) it had decided to give partial access to the requested records.
11. On April 29, 2005 IBM requested that the Respondent, the Information and Privacy Commissioner for British Columbia (the "Commissioner"), review the Ministry's decision to partially disclose the requested records (the "Third Party Review"). IBM took the position that section 21 prevented the disclosure of some information in the Agreement that the Ministry proposed to disclose to the Applicant.
12. On or about October 3, 2010 the Commissioner issued a notice of inquiry in relation to the Third Party Review. That document provided that notice to the Ministry, FIPA and IBM that, under Part 5 of FOIPPA, the Commissioner or his delegate ("adjudicator") will conduct a written inquiry on the dates set out therein.
13. On or about July 24, 2008 the Commissioner issued a preliminary decision during the Third Party Review that required the Ministry to disclose to FIPA the information in the requested records that was not at issue in the Third Party Review and was not subject to one of the exceptions in FOIPPA. The Supreme Court of British Columbia upheld that preliminary decision on December 10, 2019.
14. On or about January 11, 2010 the Ministry provided its final response to FIPA in relation to its request for the Agreement. In that response, the Ministry withheld information from the Agreement under the following sections of the Act: 15(1)(k) (harm to the security of a system), 17 (harm to the financial or economic interests of a public body or the Province), 21 (third party financial harm) and 22 (harm to personal privacy).
15. The Office of the Commissioner issued a Notice of Inquiry and Portfolio Officer's Fact Report to the Ministry, FIPA and IBM on May 27, 2010 which stipulated that the Commissioner or his delegate would consider whether the Ministry was authorized or required, as the case may be, to refuse access to information severed under sections 15, 17 and 21 of FOIPPA ("the Inquiry").
16. The Inquiry ran jointly with the third party review inquiry and was conducted by way of written submissions.

17. During the Inquiry the Ministry tendered the affidavit of David I Campbell, Director, IT Security Operations, Division Support Services, Shared Services, Ministry of Citizens' Services. That affidavit provided evidence to the effect that the disclosure of the information severed from the Agreement under section 15(1)(l) of FOIPPA, in whole or part, decreases the security of the computer systems in that, possession of the information would assist a potential hacker in attacking those systems and provide hackers with tools for attacking the computer systems that they otherwise wouldn't have. For each of the categories of information sought, Mr. Campbell provided evidence of how the release of the information would provide critical tools for hackers to attack the computer systems.

The Decision

18. In Order F10-39, the Commissioner's delegate held that the Ministry had not met its burden of proving a reasonable expectation that the disclosure of the disputed information would result in the harm identified in section 15(1)(l) of FOIPPA. The Delegate applied a test that required the Ministry to provide evidence that disclosure of the information sought to be withheld by the Ministry would, more likely than not, result in a successful breach of the entire security system, and hence result in access by the hacker to the Province data. The delegate concluded that, since the Ministry did not provide that evidence to that standard, the Ministry had failed to meet the test for refusing to disclose information under s. 15(1)(l) of FOIPPA.
19. At present, the only portions of the Agreement that the Ministry has not agreed to produce to FIPA are those portions that the Ministry has withheld pursuant to section 15(1)(l) of FOIPPA—documents the disclosure of which the Ministry expects would harm the security of the computer systems.

Part 3: LEGAL BASIS

1. This Petition is brought pursuant to the *Judicial Review Procedure Act*, R.S.B.C. 1996, c. 241 and Rules 16-1 and 20-4 of the Supreme Court Civil Rules.

Grounds for Judicial Review

2. The basis upon which this application for judicial review is brought is that the delegate of the Information and Privacy Commissioner, in concluding that the Ministry is not entitled to refuse to disclose the information under s. 15(1)(l) of FOIPPA, committed errors of law and errors of mixed fact and law resulting in a decision that not supported by law.
3. More specifically, the delegate of the Information and Privacy Commissioner ("the delegate") erred as follows:

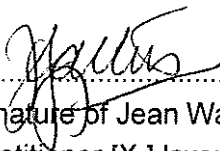
- (1) by not carrying out a proper or any analysis of the interpretation of the relevant provisions of section 15(1)(l), including the terms "security of ..a computer system" and "harm" to that security.
- (2) in his articulation of the "harm" at stake by disclosure of the information;
- (3) in failing to take into account properly or at all the relevant context of the Ministry's claim under s. 15, with respect to security controls in the circumstances. The context includes, *inter alia*, the context created by the Ministry's obligations to provide reasonable security of personal information under s. 30 of *FOIPPA* and other statutory provisions relating to obligations for the protection of personal information, the nature of security of electronic data and the fact that that it is multi-layered and multi-faceted for the management of privacy risks, the contractual obligations of the parties to the Master Services Agreement with respect to the security for the protection of information in the circumstances, the direction of the Information and Privacy Commissioner to use best practices for the security of electronic personal information and the particular sensitivity of the personal information that is protected by the computer system.
- (4) in his selection of the appropriate test and evidentiary requirements for the reasonable expectation of harm to the security of a computer system, as referred to in the opening words of s. 15 and subsection 15(1)(l) by failing to take into account adequately or at all the sensitivity of the information contained on the computer system;
- (5) in his application of the appropriate test and evidence required for the Ministry to meet the test under s. 15(1)(1) in the context of the personal information contained within the computer system.
- (6) by failing to provide reasons for his decision that would demonstrate justification, transparency and intelligibility for the decision;
- (7) by these errors, making a determination that did not fall within the range of possible, acceptable outcomes which are defensible in respect of the facts and law.

Part 4: MATERIAL TO BE RELIED ON

1. Affidavit #1 Marilyn Ackerman sworn January 11, 2011
2. *in camera* documents submitted to the Office of the Information and Privacy Commissioner.

The petitioner estimates that the hearing of the petition will take 2 days.

Date: January 11, 2011



 Signature of Jean Walters
 petitioner lawyer for petitioner

<p><i>To be completed by the court only:</i></p> <p>Order made</p> <p><input type="checkbox"/> in the terms requested in paragraphs of Part 1 of this petition</p> <p><input type="checkbox"/> with the following variations and additional terms:</p> <p>.....</p> <p>.....</p> <p>.....</p>	
<p>Date:</p> <p>.....[dd/mmm/yyyy].....</p>	<p>.....</p> <p style="text-align: center;">Signature of <input type="checkbox"/> Judge <input type="checkbox"/> Master</p>

No.
Victoria Registry

In the Supreme Court of British Columbia

Between

Ministry of Citizens' Services

Petitioner

and

Information and Privacy Commissioner of British Columbia,
IBM Canada Limited, and
BC Information and Privacy Association

Respondents

PETITION TO THE COURT

JEAN WALTERS
Ministry of Attorney General
Legal Services Branch
1001 Douglas Street
Victoria, BC
V8W 9J7
Telephone: (250) 356-8894
Fax: (250) 356-9154