

Submission to the ATIPPA Review **Commission June 2014**

Sequence of events with respect **to ATIPPA request to our town:**

In the fall of 2012 I made an ATIPPA request to the town council for information of whether or not a particular amount had been paid to a town resident. As this was an accounts payable item, it is, as far as I know, public information - I could have gone to the town office and asked for it. The weather was getting cold and I am not independently mobile, I decided it was easier for me to ask for the information as an ATIPPA request. I did this. The sequence of events that followed is listed below.

Nov. 2012: ATIPPA request for confirmation of amount paid to a resident by our town.

Dec. 2012: response received from the town. It said that they 'unable to confirm or deny' that this had been paid, quoting Section 12 (C) of the Access to Information and Privacy Act as their reason.

Jan. 16, 2013: I talked to a former manager of our town, as I thought he would know if I had been answered appropriately. He told me that he thought the town had misinterpreted that section of the act.

Jan. 21, 2013: I decided my next step was to consult the Office of the Privacy Commissioner. I spoke to a representative there who indicated that they would probably say that the town had not responded appropriately. They

gave me the information I needed on putting in a request to them, which I did.

Feb. 25, 2013: I started checking the status of my request to the Privacy Commissioner.

Mar. 4, 2013: The person to whom I spoke at the Privacy Commissioner's office seemed to agree that I should have received the information. They sent a letter to our town.

Mar. 12, 2013: The town's response to this letter was that they were standing by their original position. I then asked for a formal review by the Commissioner and prepared the information needed for submission.

Mar. 22, 2013: I mailed my submission to the Privacy Commissioner. It was due by Mar. 29, 2013.

May 10, 2013: I left a message at the Privacy Commissioner's office asking for an update.

May 14, 2013: I talked to an individual at the Commissioner's office and was told the following. The Commissioner was doing a report. This would take a while as he had two or three others to do; and this was the first time, it seems, that this section of the Act has been invoked, at least here. I was told that I should receive the report by the end of May.

June 10, 2013: I got my copy of the report from the Privacy Commissioner. The town then had 15 days to respond to me and to the Privacy Commissioner. If they still refused to provide the information I had requested, then I would have 30 days to decide about taking it to the Supreme Court.

June 14, 2013: I questioned the Commissioner's office about the town's submission to them having been 'in camera'. They were entitled to do so, but I expressed my concern with respect to the implications should this ever reach the court stage.

June 17, 2013: I received an email from the town clerk with an electronic copy of the town's letter to me and of the document I had requested.

To summarize, it took about six months to get a piece of information that was publicly available. It also has required a town resident having to go to the Office of the Privacy Commissioner to get a simple document that under law should be readily available to him or her; and the threat of that resident needing to take it to the Supreme Court if the town had still refused to provide the information requested.

Comment [1]:

My concerns are that this was a lot of unnecessary time, effort, and money because someone in a town office did not, apparently, understand the Privacy Act. My point in bringing it to your attention is my hope that you may be able to take steps to prevent such wastes of time occurring again. Do the staff of such offices need more or better training on the correct use and interpretation of the Act? Could a list what information a public office should be able to provide without question be developed?

(Mrs) Emir Anne Andrews

Portugal Cove-St. Philip's NL → Section 30(1)
Phone: [REDACTED]
Email: [REDACTED]



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report A-2013-010

June 7, 2013

The Town Of Portugal Cove-St. Philips

- Summary:** The Applicant requested records from the town of Portugal Cove-St. Philips (the “Town”) pertaining to a record of payment made to a named individual for a claim against the Town. The Town claimed section 12(2) of the *ATIPPA* (refusal to confirm or deny the existence of a record). The Commissioner found that section 12 was not applicable to the request, and the Town should respond to the Applicant without relying on section 12(2).
- Statutes Cited:** *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1, as amended, s. 12.
- Authorities Cited:** *Dagg v. Canada (Minister of Finance)* 1997 CanLII 358 (SCC); *Ontario (Minister of Health and Long-Term Care) v. Ontario (Information and Privacy Commissioner)*, 2004 CanLII 43693 (ONCA); Ontario OIPC Orders PO-1810, MO-1184, M-1160, and MO-2040; Northwest Territories OIPC Review Recommendation 09-078; British Columbia OIPC Order F10-44.

I BACKGROUND

- [1] Pursuant to the *Access to Information and Protection of Privacy Act* (the “*ATIPPA*”) the Applicant submitted an access to information request on November 29, 2012 to the Town of Portugal Cove-St. Philips (the “Town”) for a “record of accounts payable from October 2011 to February 2012.” This request was subsequently narrowed on December 14, 2012 to specifically request the “record of payment made to [named individual] for a claim against the Town.”
- [2] On December 18, 2012, the Town informed the Applicant that pursuant to section 12 (2) of the *ATIPPA*, it was unable to confirm or deny the existence of the requested record and notified the Applicant of the right to seek a review by the Information and Privacy Commissioner of this refusal of access. In a Request for Review received at this Office on January 22, 2013 the Applicant asked that this Office review the Town’s decision.
- [3] Attempts to resolve this Request for Review by informal resolution were not successful, and by letters dated March 13, 2013, the Applicant and the Town were advised that the Request for Review had been referred for formal investigation pursuant to subsection 46(2) of the *Access to Information and Protection of Privacy Act* (“*ATIPPA*”). As part of the formal investigation process, both parties were given the opportunity to provide written submissions to this Office in accordance with section 47.

II PUBLIC BODY’S SUBMISSION

- [4] The Town notified this Office on March 26, 2013 that it was maintaining the position set out in previous correspondence to this Office, which was submitted “in camera.”

III APPLICANT’S SUBMISSION

- [5] The Applicant provided a submission dated March 20, 2013. In her submission, she states that she believes that she has a right to have access to the requested information as it is a payment made

with tax dollars. As such, the Applicant believes this information should be available to her, under the *ATIPPA*, and under section 215 of the *Municipalities Act*, which states that certain documents shall be available for public inspection, including financial statements, contracts and all other documents tabled or adopted by council at a public meeting.

IV DISCUSSION

[6] In this case, the Town has refused to confirm or deny the existence of the requested information. This section reads as follows:

12 (2) Notwithstanding paragraph (1)(c), the head of a public body may in a response refuse to confirm or deny the existence of

(a) a record containing information described in section 22 ;

(b) a record containing personal information of a third party if disclosure of the existence of the information would disclose information the disclosure of which is prohibited under section 30 ; or

(c) a record that could threaten the health and safety of an individual.

[7] In *Dagg v. Canada (Minister of Finance)*, the Supreme Court of Canada considered the purpose of the federal *Access to Information Act* (the “*ATIA*”) but also commented on the important role that freedom-of-information legislation plays more generally in Canada:

The overarching purpose of access to information legislation ... is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process and secondly, that politicians and bureaucrats remain accountable to the citizenry ...

Parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on; nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view. Access laws operate on the premise that politically relevant information should be distributed as widely as possible ...

Rights to state-held information are designed to improve the workings of government; to make it more effective, responsive and accountable. Consequently, while the ATIA recognizes a broad right

of access ... it is important to have regard to the overarching purposes of the Act in determining whether an exemption to that general right should be granted.

[8] As the Assistant Commissioner for Ontario stated in Order PO-1810:

A requester in a section 21(5) situation is in a very different position from other requesters who have been denied access under the Act. By invoking section 21(5), the Commission is denying the requester the right to know whether a record exists, even when one does not. This section provides institutions with a significant discretionary power that should be exercised only in rare cases [Order P-339].

[9] The above noted factors are important in any determination of whether a public body has properly invoked section 12(2), and they weigh heavily in my consideration of this matter. Of the three subsections in section 12(2), the only one that may be applicable in this case is section 12(2)(b). Personal information is defined in section 2 of the *ATIPPA* as follows:

- o) "personal information" means recorded information about an identifiable individual, including
- (i) the individual's name, address or telephone number,
 - [...]
 - (vii) information about the individual's educational, financial, criminal or employment status or history...

[10] The Ontario Court of Appeal, in *Ontario (Minister of Health and Long-Term Care) v. Ontario (Information and Privacy Commissioner)* affirmed the decision of Ontario's Assistant Commissioner in Order PO-1810, who, in considering the equivalent section in the Ontario legislation stated:

An institution relying on this section must do more than merely indicate that the disclosure of the record would constitute an unjustified invasion of personal privacy. It must provide sufficient evidence to demonstrate that disclosure of the mere existence of the requested records would convey information to the requester, and that the disclosure of this information would constitute an unjustified invasion of personal privacy (Orders P-339 and P-808 (upheld on judicial review in Ontario Hydro v. Ontario (Information and Privacy Commissioner), [1996] O.J. No. 1669, leave to appeal refused [1996] O.J. No. 3114 (C.A.))

Therefore, in order to substantiate a section 21(5) claim, the Ministry must provide sufficient evidence to establish that:

1. *Disclosure of the records (if they exist) would constitute an unjustified invasion of personal privacy; and*
2. *Disclosure of the fact that records exist (or do not exist) would in itself convey information to the requester, and the nature of the information conveyed is such that disclosure would constitute an unjustified invasion of personal privacy.*

[11] In this case, the request was for information about the amount paid to a named third party in settlement of a claim against the Town. Given the above noted definition, the request clearly encompasses the personal information of a third party, as the record, if it exists, would contain the Third Party's name, and arguably, information about the Third Party's financial status or history, as the request is for a record of a payment made to the Third Party by the Town.

[12] Next, applying the Ontario test, we must consider whether the disclosure of the information, if it exists, would be prohibited under section 30. Section 30 reads as follows:

30. (1) The head of a public body shall refuse to disclose personal information to an applicant where the disclosure would be an unreasonable invasion of a third party's personal privacy.

(2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy where

- (a) the applicant is the individual to whom the information relates;*
- (b) the third party to whom the information relates has, in writing, consented to or requested the disclosure;*
- (c) there are compelling circumstances affecting a person's health or safety and notice of disclosure is mailed to the last known address of the third party to whom the information relates;*
- (d) an Act or regulation of the province or of Canada authorizes the disclosure;*
- (e) the disclosure is for a research or statistical purpose and is in accordance with section 41;*
- (f) the information is about a third party's position, functions or salary range as an officer, employee or member of a public body or as a member of a minister's staff;*
- (g) the disclosure reveals financial and other details of a contract to supply goods or services to a public body;*
- (h) the disclosure reveals the opinions or views of a third party given in the course of performing services for a public body, except where they are given in respect of another individual;*
- (i) public access to the information is provided under the Financial Administration Act ;*
- (j) the information is about expenses incurred by a third party while travelling at the expense of a public body;*
- (k) the disclosure reveals details of a licence, permit or a similar discretionary benefit granted to a third party by a public body, not including personal information supplied in support of the application for the benefit;*
- (l) the disclosure reveals details of a discretionary benefit of a financial nature granted to a third party by a public body, not including*
 - (i) personal information that is supplied in support of the application for the benefit,*
 - or*

- (ii) *personal information that relates to eligibility for income and employment support under the Income and Employment Support Act or to the determination of income or employment support levels;*
 - (m) *the personal information is about an individual who has been dead for 20 years or more; or*
 - (n) *the disclosure is not contrary to the public interest as described in subsection (3) and reveals only the following personal information about a third party:*
 - (i) *attendance at or participation in a public event or activity related to a public body, including a graduation ceremony, sporting event, cultural program or club, or field trip, or*
 - (ii) *receipt of an honour or award granted by or through a public body.*
- (3) *The disclosure of personal information under paragraph (2)(n) is an unreasonable invasion of personal privacy where the third party whom the information is about has requested that the information not be disclosed.*
- (4) *A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy where*
- (a) *the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation;*
 - (b) *the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation;*
 - (c) *the personal information relates to employment or educational history;*
 - (d) *the personal information was collected on a tax return or gathered for the purpose of collecting a tax;*
 - (e) *the personal information consists of an individual's bank account information or credit card information;*
 - (f) *the personal information consists of personal recommendations or evaluations, character references or personnel evaluations;*
 - (g) *the personal information consists of the third party's name where*
 - (i) *it appears with other personal information about the third party, or*
 - (ii) *the disclosure of the name itself would reveal personal information about the third party; or*
 - (h) *the personal information indicates the third party's racial or ethnic origin or religious or political beliefs or associations.*
- (5) *In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body shall consider all the relevant circumstances, including whether*
- (a) *the disclosure is desirable for the purpose of subjecting the activities of the province or a public body to public scrutiny;*
 - (b) *the disclosure is likely to promote public health and safety or the protection of the environment;*
 - (c) *the personal information is relevant to a fair determination of the applicant's rights;*
 - (d) *the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;*
 - (e) *the third party will be exposed unfairly to financial or other harm;*

- (f) the personal information has been supplied in confidence;*
- (g) the personal information is likely to be inaccurate or unreliable;*
- (h) the disclosure may unfairly damage the reputation of a person referred to in the record requested by the applicant; and*
- (i) the personal information was originally provided to the applicant.*

[13] There is nothing in section 30(2) that tells us that disclosure of the requested information, if it exists, is not an unreasonable invasion of privacy. Likewise, we can also take no guidance from section 30(3) or (4) that disclosure would be an unreasonable invasion of privacy. Therefore, having accepted that the information (if it exists) would constitute personal information, we must consider all of the circumstances, including the factors set out in section 30(5), to determine whether disclosure of the requested information, if it exists, would be an unreasonable invasion of privacy and therefore not subject to disclosure under section 30(1). The general principle that public bodies should be accountable to the public for expenditure of public funds, including payments to individuals goes to the heart of the purpose of access to information legislation and weighs heavily in favour of disclosure.

[14] Across the country, Commissioners have found that one time payments made to citizens by a public body in settlement of legal claims do not constitute an unreasonable invasion of privacy, even where settlement resulted from arguably sensitive personal matters, such as claims for wrongful dismissal or other employment issues (i.e. Ontario Order MO-1184, Northwest Territories Review Recommendation 09-078), human rights complaints (i.e. Ontario Order M-1160), claims made by a former employee against former co-workers (i.e. British Columbia Order F10-44), and claims made against police agencies (i.e. Ontario Order MO-2040).

[15] Based on the “in camera” submissions of the Town and the results of the research carried out by an Analyst from this Office, I have determined that disclosure of the information requested, if it exists, would not be an unreasonable invasion of privacy, as it is desirable for subjecting the activities of the public body to public scrutiny, as set out in section 30(5)(a).

VII CONCLUSION

[16] Given my finding above that disclosure of the requested information, if it exists, would not be an unreasonable invasion of privacy, I need not consider the second part of the test under section 12(2). As both parts of the test must be met in order to properly invoke section 12(2), it is my finding that section 12(2) was not properly invoked by the Town.

VIII RECOMMENDATIONS

[17] Under the authority of section 49(1) of the *ATIPPA*, I recommend that the Town respond to the Applicant's access request again, not relying on section 12(2).

[18] Under the authority of section 50 of the *ATIPPA*, I direct the head of the Town to write to this Office and the Applicant within 15 days after receiving this Report to indicate the final decision of the Town with respect to this Report.

[19] Please note that within 30 days of receiving the decision of the Town under section 50, the Applicant may appeal that decision to the Supreme Court of Newfoundland and Labrador Trial Division in accordance with section 60 of the *ATIPPA*.

[20] Dated at St. John's, in the Province of Newfoundland and Labrador, this 7th day of June 2013.

E. P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador