SUBMISSIONS OF THE INFORMATION AND PRIVACY COMMISSIONER

COMPREHENSIVE REVIEW OF THE ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT

CONSULTATION PAPER
October 13, 2015

December 21, 2015

1. INTRODUCTION TO THE ACT

1.1 SCOGO: has recommended that the government and other public bodies should be more proactive in the disclosure of records and move towards proactive disclosure policies and an "access by design" approach to records.

The Government of the Northwest Territories (GNWT) has previously indicated to the Standing Committee on Government Operations its support for Access by Design principles. The Government recognizes that there is an increased expectation that public bodies will disclose information with openness and transparency while still ensuring personal and sensitive information is appropriately protected. Principles, such as Access by Design, encourage public bodies to take a proactive approach to releasing information, making the disclosure of GNWT information a priority where possible.

Recently, the Government of Newfoundland and Labrador (NFLD) revised their Access to Information and Protection of Privacy Act indicating that one of the primary purposes of the legislation is to "facilitate democracy through ensuring the citizens have the information required to participate meaningfully in the democratic process". In support of this purpose, they have limited the application of discretionary exceptions in those instances where the public interest in disclosure clearly outweighs the reason for the exception.

These amendments signal that public bodies have a responsibility to be more proactive in disclosing information. Information held by public bodies should be readily disseminated and not simply provided in response to a formal access to information request. When a request is made, the public body must take into account the public's interest in the information and weigh it against any exceptions.

Do you support legislative amendments that would require public bodies to be more proactive in the disclosure of records? Or do you feel that proactive disclosure could be facilitated through policies and programs?

Pro-active disclosure should absolutely be encouraged and supported by legislation. While there are some pieces of legislation that, in a limited way, provide for disclosure of records, there is nothing in the *Access to Information and Protection of Privacy Act* (ATIPPA) that requires public bodies to pro-actively make information available. Some public bodies are making some strides (for example in the posting of procurement information) but the commitment to proactive disclosure is uneven. Furthermore, there is still a lot of work to do within government to change the culture of protectiveness and secrecy that tends to pervade government generally. Changes in attitudes will not happen with “policies and programs” alone. Most other jurisdictions now have some form of legislation which requires disclosure of certain information. For example, many jurisdictions now have a published “Sunshine List” which lists the names and pay for all employees earning over a given base salary (in most cases, over $100,000.00 per annum). I **recommend** that amendments be made to the *Access to Information and Protection of Privacy Act* which would require public bodies to pro-actively disclose certain, specific types of information, such as factual material, statistical surveys, public opinion polls, environmental impact statements, procurement information, and other records often of interest to the public. In addition, I **recommend** that amendments address the disclosure of incomes of public servants earning incomes over a stated

amount, as well as the pro-active disclosure of information such as employee travel costs. This would bring the Northwest Territories in line with most other Canadian jurisdictions.

In addition to the requirement of "proactive" disclosure, however, public bodies should be required, where requested, to be able to provide access to records in machine-readable formats so that the Applicant can have access to and easily use databases and data sets (provided that personal information is protected). The US Federal Freedom of Information Act was amended almost 10 years ago to provide for the disclosure of records in electronic form. At the time it was noted:

> [T]he information technology currently being used by executive departments and agencies should be used in promoting greater efficiency in responding to FOIA requests. This objective includes using technology to let requesters obtain information in the form most useful to them.

Most work done by public bodies today is recorded and retained electronically. With the proper redaction software, disclosure of records in electronic format would significantly reduce the time and effort necessary for disclosure. Furthermore, it would result in the records being provided to the Applicant in a format which is likely going to be far more useful to him/her than a paper record. I **recommend** that the Act be amended so as to require that, where the record exists in electronic form and the public body can reasonably provide it in that form, it should disclose the record in machine-readable format.

Though perhaps an issue more properly dealt with in regulation or a general policy directive, I **recommend**, as well, amendments that would require public bodies to conduct "access assessments" and to incorporate "access by design" into new initiatives on a go-forward basis to help to ensure that the future of access to information in the Northwest Territories remains robust and up to date.

> **Do you support amending the Act to indicate the application of discretionary exceptions will not apply in instances where public interest in disclosure clearly outweighs the exceptions?(Also dealt with in discussion on 3.12 Other Exceptions to Consider)**

The discretionary exemptions in the Act need some attention.

The "public interest" override issue was thoroughly discussed in Chapter 3 of Volume II of the "Report of the 2014 Statutory Review, Access to Information and Protection of Privacy Act, Newfoundland and Labrador" (the Newfoundland Report). I would refer you to the discussion in that report as being very helpful. As noted at page 73, the Supreme Court of Canada recently discussed the issue in *Criminal Lawyers' Association* [2010] 1 SCR 815 (para 66)and made the following observations:

> As discussed above, the "head" making a decision under ss. 14 and 19 of the Act has a discretion whether to order disclosure or not. This discretion is to be exercised with respect to the purpose of the exemption at issue and all other relevant interests and considerations, on the basis of the facts and circumstances of the particular case. The decision involves two steps. First, the head must determine whether the exemption applies. If it does, the head must go on to ask whether, having regard to all relevant interests, **including the public interest in disclosure**, disclosure should be made.[emphasis added]

The authors of the Newfoundland Report came to the following conclusion on this point:

> The Committee concludes that in a modern law and one that reflects leading practices in Canada and internationally, it is necessary to broaden the public interest override and have it apply to most discretionary exemptions. This would require officials to balance the potential for harm associated with releasing information on an access request against the public interest in preserving fundamental democratic and political values. These include values such as good governance, including transparency and accountability: the health of the democratic process; the upholding of justice; ensuring the honesty of public officials; general good decision making by public officials.

I **adopt the recommendations** made in the Newfoundland Report with respect to this issue. They can be found at page 79 of that report.

Quite apart the "public interest override" issue, I **recommend** that amendments be made to the discretionary exemption sections of the Act to clarify that disclosure is always the default position, even when a record meets the criteria for a discretionary exemption. As a matter of public policy all records should be disclosed unless there is a real reason not to. As the Act is currently written, there is a two part process involved in the application of discretionary exemptions - 1. Determining whether the record qualifies for the exemption and 2. Exercising the discretion taking into consider all the relevant circumstances. Most public bodies stop at the first step and simply refuse to disclose a record which falls within the criteria for the exemption. Amendments should be made to make it clear that all records subject to a discretionary exemption are to be disclosed as the default position and only if the public body can clearly articulate a good reason for withholding the record should access be denied.

1.2 With the exception of the definition of employee, our current list of definitions has not been updated since the Act came into force.

One issue that was identified in the review relates to the definition of personal information. Currently, an individual's business address or business telephone is considered personal information. A number of jurisdictions have removed this reference.

Do you support amending the legislation to remove reference to business information?

The definition of "personal information" in the definitions section of the Act is not all inclusive. Whether "business address and business telephone number" are included in the definition does not change the nature of the information. It IS personal information. Just as the absence from the definition of "email address" does not mean that an email address is not personal information for the purposes of the Act. The real issue is whether or not the disclosure of business contact information would constitute an unreasonable invasion of an individual's privacy. In most cases, it would not. That said, including "business" information under the definition of personal information does seem to result in the inappropriate redaction of this information from many records. I would, therefore, **recommend** that the definition of "personal information" be amended to remove reference to business contact information, and to include email addresses and other electronic contact information.

Do you believe the current listings of definitions need to be updated? If yes, do you have definitions you would like to see included or removed?

I **recommend** under the definition of "personal information", subsection (e) include a general reference to "other biometric information" about the individual, rather than just "fingerprints", "bloodtype" or "inheritable characteristics".

I **recommend** that the definition of "record" be updated to include a specific reference to electronic records, data and data sets.

I **recommend** that the definition of "law enforcement" be changed by removing (b) and (c) under that definition and including instead a more specific provision, such as the following:

> b) investigations or proceedings conducted under the authority of or for the purpose of enforcing an enactment which lead to or could lead to a penalty or sanction being imposed under the enactment

The current definition is far too broad and suggests that any action that might end in a sanction or penalty is included, even though the "law enforcement" exception is clearly focussed on criminal and/or quasi-criminal proceedings.

1.3 The current list of records that are excluded from the application of the Act has not been reviewed since the Act came into force. We believe the listing should be assessed to determine if excluding these categories of records is still required and if other categories of records held by public bodies should be identified as outside the scope of the Act.

Possible examples that could be considered for exclusion:

- ***personal or constituency records of a member of the Legislative Assembly;***
- ***quality assurance records as defined by the Evidence Act;***
- ***health information as defined by the Health Information Act,(HIA) which is under the custody or control of a public body that is a custodian as defined by the HIA.***

Do you believe the current list of record categories should continue to be excluded from the application of the Act?

As noted by Suzanne Legault, the Federal Information Commissioner in her presentation to the review panel in Newfoundland and Labrador:

> I really do believe strongly and I agree with Commissioner Ring [the Newfoundland and Labrador IPC] when he says whenever – whenever we want to carve out exceptions to the general application of the access Acts...there has to be a very, very strong policy case made that this is absolutely necessary in that in fact the general provisions under the Act cannot apply appropriately. (Report Pg 129)

None of the existing exclusions in section 3 of the current Act have been much of an issue in any review conducted by my office since the coming into force of the Act and there are good public policy reasons for the exclusions. I would not advocate for the removal of any of them. I would, however, suggest that 3(1)(d) be clarified. It has been suggested in at least one case that interview questions routinely asked during job interviews fall under this category. In my opinion, interview questions do not amount to a "test" or "examination". Rather, the ordinary meaning of the term should apply - tests given in school, tests for learners drivers licenses etc. Clarification of this would be helpful.

Are there categories of records you believe should be included? If yes, what are they and why?

The discussion paper included with this consultation suggests the possible addition of other exclusions:

- personal or constituency records of a member of the Legislative Assembly
- quality assurance records as defined by the *Evidence Act*
- health information as defined by the *Health Information Act (HIA)* which is under the custody or control of a public body that is a custodian as defined by the HIA

I see no reason to add any of these to the list of excluded records. In the history of the Act, I have yet to deal with a request for the personal or constituency records of a member of the Legislative Assembly. It seems to me, in any event, that constituency records could easily be dealt with within the existing provisions of the Act in that they are not in the custody or control of a public body. Quality assurance records are fully covered under the new *Health Information Act* (HIA) which in turn has provisions which describes the interplay between the ATIPPA and the HIA. Adding these categories of records as "excluded" from ATIPP will simply serve to muddy the waters. I **recommend** against adding any more exclusions under the Act.

I do, however, **recommend** an amendment which would make it clear that should an issue arise with respect records for which an exclusion is raised, the Information and Privacy Commissioner be granted clear and unfettered authority to require production of the records in question to evaluate the claim being made.

1.4 Currently, there are no set criteria for determining what acts or sections of acts should be outside of the ATIPP Act. There is also no requirement to identify in regulations the different NWT Acts that are "notwithstanding" to ATIPP. This is a practise that has been taken by some jurisdictions.

Do criteria need to be developed that will assist Departments who are developing legislation determine if an act or sections of the Act should be "notwithstanding" to ATIPP? Should these criteria be set out in legislation or established by policy?

Paramountcy provisions remove access and privacy rights. As Former Alberta IPC Frank Work stated in this Office's 2011 study of paramountcy clauses that override the FOIP Act:

> Left unchecked, the practice of taking other enactments out of FOIP by making them "paramount" to FOIP has the potential to turn FOIP into "a piece of Swiss cheese", causing its death "by a thousand cuts" or bringing about its virtual "repeal by degrees."
> [Introduction]
>
> A number of existing paramountcy provisions may be unnecessary as the FOIP Act provides sufficient privacy protection. A mandatory requirement that proposed paramountcy provisions be submitted to me for review and comment can help in reducing the number of unnecessary paramountcy provisions. (Becoming a Leader in Access and Privacy, Submissions to the 2013 Government of Alberta FOIP Act Review, Office of the IPC of Alberta, pg 13

I adopt Former Commissioner Work's analysis and suggestion and **recommend** that there be an amendment to the Act which would require that any proposed paramountcy provision in new or amending legislation be submitted to the IPC for review and comment.

In terms of guidelines for when such provisions are included in legislation, guidelines would be useful. A good starting point would be the establishment of policies but the longer term goal should perhaps be to include them in the legislation itself. In the meantime, a requirement that any such provisions in new legislation be reviewed by the IPC will at least ensure that due consideration is given before such provisions become law.

Should a listing of NWT Acts that include "notwithstanding to ATIPP" provisions be identified in the Regulations?

While this might be helpful, I would suggest that this information might be better placed in the ATIPP Directory, as the list changes fairly often.

2. ADMINISTRATION OF THE ACT

2.1 It is standard practise to protect the identity of an applicant who has initiated an access to information request throughout the processing of that request. Access and Privacy Coordinators, share the identity of a requestor within their public body on a need to know basis only.

Recently, NFLD added a provision in their legislation that requires public bodies to anonymize the identity internally, until the final response is sent to the requestor. This does not apply to requests for personal information where the identity of the applicant is necessary in order to process the request.

Do you believe that our legislation should be amended to protect the identity of an access to information applicant from disclosure, during the ATIPP process? If yes, why?

As noted in the consultation paper, it is my understanding that the identity of the individual making an access to information request is protected as a matter of policy and practice. There are a number of good reasons for such an approach. The first is that the general spirit and intention of the Act which dictates that when the Applicant is an individual, they have the right to privacy as granted under the Act. This, however, would apply only to an "individual" applicant. There are no privacy rights granted to corporate entities under the Act. The second reason, however, is to prevent political interference in access requests. In Newfoundland and Labrador the legislation now protects the identity of the Applicant because there was evidence of significant political interference in some ATIPP requests. The Commission which prepared the Newfoundland Report noted:

> This process of focussing on the identity of the requester rather than the merit of the request may account for the delays experienced by media and opposition parties.....

> Two observations can be made here. The first is that the time spent on certain categories of requesters perceived as problematic through prior identification adds to delays and negates the duty to assist.
>
> The second observation is that the current system, where requests are scrutinized by staff, the deputy minister, and often the minister, facilitates the interpretation of ATIPPA in a partisan political way rather than in a fair, principled way.

Newfoundland and Labrador is not the only Canadian jurisdiction that has had to deal with this kind of political interference. It appears to be a problem in a number of jurisdictions. While this has not yet manifested itself as a problem in the Northwest Territories, the possibility certainly exists, particularly where the issue might be of significant political sensitivity. I therefore **recommend** the inclusion of a provision which would limit the disclosure of the name of the Applicant in the ATIPP process.

2.2 SCOGO: the GNWT review its fee schedule to ensure it does not place an undue cost on persons requesting access to information.

> ***Access and privacy legislation is intended to give individuals the right of access to general information held by public bodies as well as the right to access their own personal information or request a correction to it. Therefore, it's important that the fee structure relating to accessing information does not become a deterrent to access. However that does not mean it's unreasonable to charge fees, as they can assist in discouraging frivolous requests.***
>
> ***The following table (Table 1.) below details the typical fees charged in relation to general and personal access to information requests, across Canada. A number of jurisdictions have lowered or eliminated the initial application fees for general requests and photocopying fees have been decreased. While some jurisdictions have increased the hourly fees relating to locating and preparing records, this has been somewhat offset by an increase in the number of "free" hours applicants may get.***

Following a review of the attached fee table, are the current fee requirements still appropriate?

There is a very good review of the “fees” issue in the Newfoundland Report at pages 51 to 58, which I have attached as an Appendix to this submission. From my perspective, the current fee structure is cumbersome, unclear, dated and somewhat inconsistently applied.

The issue here is what is the intention of imposing fees? Fees should not be used to frustrate or discourage access to information requests. The spirit and intention of the legislation is to allow access, not place barriers in the way. If fees are to be part of the legislative scheme, then, they must be reasonable and not such that they will deter applicants. As noted in the Newfoundland Report:

> Any change related to fees and charges should facilitate, not frustrate access. Changes should make the *Act* more, rather than less, user friendly. (Page 57)

It has always been acknowledged that the fees structure under the *Act* is not intended to achieve full cost recovery. In fact, I would venture to guess that the real cost of administering the $25.00 application fee alone is greater than the $25.00 received, making for a net loss, before we even get to the point of starting to respond to the request. The only real purpose of the fees, then, would be to act as a check/balance to those who would abuse the system and application fees are of limited assistance in this regard.

The current $25.00 "Application Fee" for access to information requests for general information is at the top of the scale nationally (application fees range between $0 and $25.00). There is no application fee for someone seeking his or her own personal information.

The expert panel reviewing the Newfoundland and Labrador Act concluded that there is "little merit in retaining the application fee" (page 57). I **recommend** that the Application Fee be eliminated.

In terms of the fees for searching for and responding to access requests, our act currently provides for what amounts to five and a half hours of "free" processing time before the additional fees kick in. There is a significant amount of confusion over the way in which this time is calculated. In the Newfoundland Report, the Committee recommended that:

> It makes sense to lengthen the "free search" period from four hours to 15 hours.....The only time that would count toward processing charges would be the direct searching time for the records. Time spent narrowing the request with an applicant would not count toward the free time allotment, and neither would the time spent to determine if exemptions should apply.

I suggest that 15 hours is a much better benchmark than the current 5.5 hours and **recommend** that change. I also **recommend** that amendments be made to make it clear that only the time spent actually searching for records can be considered for calculating both the "free" time and the "fee" time. The current wording of the regulations in this regard is very unclear and, in fact, appears to be internally contradictory.

Are the current fee provisions and fee schedule clear and understandable?

The fee schedule is decidedly not "clear and understandable". In fact, there are internal inconsistencies that have been the focus of a number of fee review requests over the years. I **recommend** that the regulations be amended so that it is clear what can and what cannot be charged (as noted above).

I also **recommend** that the regulations be updated to reflect the realities of the form which records take in today's electronic world. For example, the Regulations currently provide for a fee for "computer processing and related charges" which may well have been a real cost factor 20 years ago, but which today is not relevant because virtually all written records are created and stored electronically. The current fees for "floppy disks, computer tapes, microfiche and microfilm" need to be reconsidered, as do those charges associated with video and audio cassettes. While these medium may still be subject to requests for information, it seems to me that in most cases, records today are more likely to be converted to an electronic format for the purposes of disclosure than to be recreated in their original format. This said, the current fee schedule does not provide a fee for disclosure of records in electronic medium. To this end, I **recommend** that the regulations reflect the costs of electronic disclosure - for example, if a jump drive or other removable apparatus is necessary, a cost can be associated with that. In the event that disclosure is entirely electronic (ie: by email) there should be no cost to the applicant. Where paper records are concerned, I **recommend** that the regulations be amended to clarify that the Applicant should only be charged for one set of records regardless of whether or not the public body has to make additional copies for their own records.

I **recommend**, as well, that the Act and Regulations continue to provide for a waiver of fees in circumstances of financial hardship and/or when for another reason it is fair to excuse payment, but that these provisions be expanded to include "where it would be in the public interest" to disclose the information. I further **recommend** that the *Act* be amended so as to provide that when the Information and Privacy Commissioner reviews a matter concerning a fee review, her determination on that issue be final.

2.3 When the Act came into force in December 1996, the procedures developed for processing formal access to information requests were based on paper records. However advances in technology have changed the way government does business and records created today are typically in an electronic format.

While public bodies in the NWT routinely provide documents to applicants in an electronic format, there is currently no direction on this in the Act. Some jurisdictions have addressed this in their legislation, while others have included this in policies.

Do you believe the Act should be amended to allow an applicant to indicate how and in what form they would prefer to access the records held by the public body?

In a perfect world, applicants should be able to receive records in a form that makes the most sense for them. Once again, the Newfoundland Report includes a good discussion about the increasing demand for records in the form requested. As noted in that report, requesters are more and more frequently seeking access to government data and data sets which they can use and manipulate themselves (in "machine readable form"). This is where "open government" initiatives come in. However, in the context of access to information, the disclosure of records and data still has to meet the requirements of the Act. As noted in the Newfoundland Report:

> Data is a dynamic commodity with tremendous economic value and social utility....Of course, even with the limitless potential for use, data and data sets have to be protected to ensure that personal information is not disclosed.

The Report recommended that the term "records" be amended to include data sets and other machine readable records, to require that disclosure of such records be subject only to the limitations applied to all other records of public bodies and that data sets be provided to requesters in re-useable format. For the Northwest Territories, I **recommend** that applicants be given the choice of the medium in which they receive their responses, where possible. This said, the reality is that not all public bodies currently have the technology which would allow for disclosure generally in electronic form, let alone the disclosure of data and data sets in machine readable form. I **recommend** that all public bodies be required to have the necessary technology to disclose records in response to a conventional access to information request electronically within a realistic time frame (5 years?). In the meantime, where the technology is already in place, I **recommend** that applicants be able to choose the form disclosure takes. Keeping an eye on the future, the Government of the Northwest Territories and public bodies have to begin to plan for more open government initiatives and creating their data and data sets in a way such that they will be able to respond to a request for "machine readable" records.

Should there be limitations on the form, possibly in regulations? For instance if requested in electronic form it could be restricted to "using the public body's normal computer hardware and software and technical expertise."

As noted above, as time marches on, there will be more and more requests for access to records in electronic form. As noted, while it makes sense to put some limitations on the form of disclosure of records, this cannot be used as a way to prevent access or put up barriers to prevent access to records. There must be some responsibility on the GNWT and its agencies to maintain reasonably current technologies and technological expertise so that "using the public body's normal computer hardware and software" does not become an excuse not to disclose certain records.

Should we consider processing a full request through electronic means, i.e. application request, payment of fees, notice or notifications, provision of records, etc.?

This should be a longer term goal. The technology is certainly available to make this possible and eventually paper records will be the exception, not the rule. That said, there would have to be appropriate protections built into how this is done because many times the records requested are full of personal information or other mandatory or discretionary exceptions to disclosure. Further, there may be applicants who do not have access to or the knowledge to use records in electronic form and this will have to be acknowledged and addressed in such a system. That said, I would **recommend** that the GNWT to begin to develop a system which would allow ATIPP requests to be dealt with "on-line" as an option.

2.4 Public bodies routinely produce records from existing information systems in response to formal access to information requests however, in some instances producing the record can be complicated and could be considered to constitute an unreasonable interference in the operations of the public body.

Currently, public bodies determine what constitutes "unreasonably interfering with the operations of the public body

Do you believe there should be criteria developed to assist public bodies assess what could be considered as "unreasonably interfering with the operations of a public body"?

It may well be of assistance to ATIPP Co-Ordinators, who are the people within public bodies tasked with the administration of the Act, to have some guidelines to refer to when making determinations pursuant to s.11 to extend the time for responding to an access to information request. In particular, set criteria would provide some consistency where the reason for the delay is that there would otherwise be an "unreasonable interference" with the operations of the public body. It would, however, be difficult, I think, to create a definitive set of rules which would appropriately apply to every public body. The fact is that every public body is different and has different

limitations. What would be a routine access request in one department might be overwhelming to another for any number of reasons. While I would not object to such an amendment, it would have to be very carefully crafted. Any such guidelines should recognize the legislated obligation to respond to applicants in a timely fashion and that ATIPP work may have to take precedence over other work before this section of the Act can be invoked.

If yes, do you believe the criteria needs to be provided for legislation or in policy?

If such criteria were to be developed, it might be better to do so in the form of regulations or policy, keeping in mind the different obstacles that might affect the response time in each public body at any particular point in time.

2.5 Concerns have been raised in the past by media, applicants and the general public regarding whether a 30 day initial response time is appropriate, however the current timeframe is in keeping with the majority of jurisdictions in Canada.

Does the initial response time of 30 days need to be revised? If yes, what is an appropriate time limit?

I do not believe that this response time needs to be revised. I do, however, **recommend** that s. 8 be reworded to make it clear that 30 days is a maximum and that all ATIPP requests should be responded to "as soon as practically possible" with an outside time limit of 30 days. I have dealt with a number of instances in which the response was ready to go out long before the end of the 30 days but, for whatever reason, was held until the last day. This is not in keeping with the spirit and intention of the Act.

I note, as well, that the combination of ss. 8 and 9 suggest that a "response" may or may not include the actual disclosure of responsive records. Section 9(1)(b) in particular suggests that there is fairly much an open ended time frame for giving access once the "response" has been provided to the Applicant. It is the general practice of most public bodies to include the responsive records with the section 8 response but I can quite easily imagine a situation in which this wording might be used as a tool to delay the actual disclosure of records. I therefore **recommend** that sections 8 and 9 be amended to make it clear that the records should accompany the response unless the Applicant has indicated that he/she wishes to view the records in the offices of the public body, in which case a time and a date for that should be provided with a specific time limit (within 10 days?).

2.6 SCOGO: has expressed concern with delays in responding to access to information requests. In a review of the matter it was determined that a number of requests, that were made during the time period referenced by Standing Committee, were past the original 30 day deadline due to time extensions.

In the NWT, public bodies may make their own determination on what constitutes a "reasonable period" for a time extensions. However, on review, it is clear that there has been an inconsistent approach on what is considered a reasonable period.

Across Canada, approaches to initiating a time extension are varied. The majority of jurisdictions have specific time frames for an initial time extensions (15 - 30 days). In some instances, a public body may set an initial time period of 30 days or with the IPC's permission, a longer time period. Other jurisdictions require public bodies to apply directly to the IPC for approval of a time extension, in particular if they have received multiple concurrent requests from the same applicant(s). Another jurisdiction indicated public bodies may seek consent of the applicant to extend the time period.

Do you believe the Act should be amended to include a set number of days for an initial time extension? If yes, how many days would you suggest?

Do you believe the Act should require that a request for a time extension be made directly to the IPC, or an applicant?

This is one area of the Act which badly needs to be amended so as to limit the length and number of extensions taken by public bodies. There have been a number of instances in which multiple extensions of time have been taken by a public body, each extension for more than 30 days, so that by the time the public body has finally met its obligations to provide access to certain records, six months or even a year have passed. This is clearly not in keeping with the spirit and intention of the Act. The requirement to ensure that extensions be for a “reasonable” period of time has lost all meaning. I **recommend** a number of amendments to the Act to address this situation:

- limit the extension public bodies are able to take pursuant to section 11 to one extension of no more than 20 days;
- require that notice of that extension be given to the Applicant no less than five business days **before** the end of the initial 30 day period, and that the notice include a statement advising that the extension can be referred to the Information and Privacy Commissioner for review;
- in the event that the public body is not able to respond within the initial 50 days, they must apply to the IPC for a further extension and that application must be made no less than five business days **prior to** the end of the extended period;
- require that the request to the IPC for a second extension include a detailed explanation as to the issues which are preventing the disclosure within the time frames outlined;
- require that public bodies continue to actively work on responses during any review by the IPC

- provide that the decision of the IPC in these cases is final (i.e. - not a recommendation, but an order)

2.7 The ATIPP Policy and Guidelines manual, states that the transfer of an access to information request to another public body, should be done quickly, however the legislation does not provide specific time frames for the transfer. This has resulted in inconsistent response times between public bodies for transferred requests.

Across Canada, the majority of jurisdictions have set out specific time frames that a public body must meet when they transfer an access to information request. The time frames range between 5-20 days.

Do you believe the Act should be amended to indicate a set time frame for transferring a request to another public body?

If yes, what period would you suggest?

It should be evident very quickly if some or all of a Request for Information received by a public body needs to be transferred to another public body for response. This determination should be made as one of the first steps in the process of responding to an ATIPP Request. I **recommend** that transfers be completed within five working days of receipt of the request.

2.8 The manner in which notice is provided is currently limited to the above noted methods, however technological innovations have changed the way we communicate with the public.

Other jurisdictions have addressed technological changes by indicating notice may be provided by facsimile or in electronic form. Alberta's legislation allows notice to be provided to individuals through electronic form if the individual the documents pertain to consents to accept the notice or document in the form. NWT legislation, such as the Residential Tenancies Act also allows for the use of fax or a method set out in the regulations, which allow for notice to be provided by email,

> ***"(2) For the purposes of subsection 71(1) of the Act, a notice or other document to be served on or given to a landlord, tenant or rental officer may be served or given by e-mail if the receiver provides his or her e-mail address to the sender for that purpose.***

Do you have concerns about providing individuals notice in a secure and confidential manner, through facsimile or electronic methods?

If yes, what are your concerns?

The reality of today's world is that most people rely heavily and extensively on "fax" and email to communicate with one another. Use of facsimile machines is, in fact, in decline as a means of communication. Both of these means of communication, and future means of electronic communication, must be used with caution as there are privacy concerns inherent which many do not recognize or consider.

This said, I see no reason that administrative matters cannot be dealt with by fax, email or any other means of communication. This would include the giving of "notice" under the ATIPP Act, particularly where the applicant has approved either explicitly or implicitly to that method of notice. I therefore **recommend** that the Act be amended to allow for the giving of notices under the Act by email, fax or other form of written communication where the Applicant has submitted his/her Request for Information by that method or has otherwise indicated his/her consent to that means of communication.

Consideration should be given to requiring communications under the Act to be encrypted when transmitted electronically.

3. EXCEPTIONS TO DISCLOSURE

3.1 SCOGO: recommendation, in situations where information is withheld, public bodies must provide a full explanation of the rationale for the decision.

The IPC has also raised concerns that public bodies are not clearly indicating the reasons why a mandatory or discretionary exception to access is being applied.

Should the Act be revised to require greater clarity on the rational for the application of mandatory and/or discretionary exceptions or should this be addressed through policies or procedures?

When dealing with discretionary exemptions under the Act, public bodies must apply a two step process. The first is to determine whether the information in question meets the criteria to qualify it for the exemption. For example, is the information subject to solicitor/client privilege or is it a cabinet confidence? If the information falls within the parameters of the exemption, the second step then is for public bodies to exercise discretion before they disclose it. It has been my position since the Act first came into effect that the rule is always disclosure and the discretion should only be applied to refuse disclosure where there are well considered and well articulated reasons for such a refusal. Unfortunately, most public bodies, even those which deal with a large volume of access to information requests, almost always stop after the first step. If the information meets the criteria for an exemption, it is not disclosed. Never have I seen a response letter to the applicant which provides an explanation by the public body of the reasons for the exercise of discretion against disclosure. In fact, rarely does a public body articulate any kind of explanation even when specifically asked for such an explanation during a review process.

I **recommend** that the Act be amended to provide that, in the case of discretionary exemptions, public bodies must advise the Applicant not only which exemption is being applied but also the specific harm that is "reasonably expected" to occur if the information is disclosed and the basis for that reasonable expectation. I further **recommend** that the Act be amended so as to specify that in the case of discretionary exemption, the starting point is that the record will be disclosed. If the record meets the

criteria for the application of a discretionary exemption it should still be disclosed unless the public body can justify non-disclosure.

3.2 ***All jurisdictions provide exceptions to the right of access in order to protect information that falls within the category of cabinet confidences however, the type of information which falls within this protection varies.***

Some jurisdictions have tried to provide clarity on what is considered a cabinet confidence by including a provision that identifies the types of cabinet information that would fall under the mandatory protection of this section.

Recently Newfoundland included a provision within this section, which defined "cabinet records" and included the following list of records considered to be cabinet confidences.

"cabinet record" means:

- ***a)*** ***advice, recommendations or policy considerations submitted or prepared for submission to the Cabinet;***
- ***b)*** ***draft legislation or regulations submitted or prepared for submission to the Cabinet;***
- ***c)*** ***a memorandum, the purpose of which is to present proposals or recommendations to the Cabinet;***
- ***d)*** ***a discussion paper, policy analysis, proposal, advice or briefing material prepared for Cabinet, excluding the sections of these records that are factual or background material;***
- ***e)*** ***an agenda, minute or other record of Cabinet recording deliberations or decisions of the Cabinet;***
- ***f)*** ***a record used for or which reflects communications or discussions among ministers on matters relating to the making of government decisions or the formulation of government policy;***
- ***g)*** ***a record created for or by a minister for the purpose of briefing that minister on a matter for the Cabinet;***
- ***h)*** ***a record created during the process of developing or preparing a submission for the Cabinet; and***
- ***i)*** ***that portion of a record which contains information about the contents of a record within a class of information referred to in paragraphs (a) to (h)."***

Is the current list of information that would disclose a confidence of Executive Council still appropriate? If no, please indicate what information you would remove or add, and why?

Should this provision be revised to further clarify what records are considered information revealing a cabinet confidence?

Our current legislation is worded quite differently from most other Canadian jurisdictions. All other Canadian jurisdictions except for Newfoundland and Labrador, the three northern Territories and the federal government refers to information or records which would “reveal the substance of cabinet deliberations”. Our legislation simply provides for an exemption of records that would “reveal a confidence” of the Executive Council. It then lists a number of broad types of records which would be included in this definition. The different wording in our current legislation suggests a

wider application of the “cabinet confidence” exception in the Northwest Territories than exists in other Canadian jurisdictions which I don’t think is intentional. Further, the subsections of section 13 (the “Executive Council” confidences section) are very broadly worded and difficult to reconcile with the historical reasons for the exclusion. The approach in Newfoundland in Labrador seems to me to be much clearer and easier to interpret. That province defines the term “cabinet record” and provides a definitive list of what that term includes (and does not include). It then provides that:

a) “cabinet records” are protected from disclosure;
b) with respect to all other records, that information in the records that would reveal the substance of Cabinet deliberations is not to be disclosed;
c) the IPC has unfettered jurisdiction to require the production of all “cabinet records” and all records which would “reveal the substance of Cabinet deliberations” for the purposes of reviews;
d) a designated individual within the executive council has the discretion to disclose cabinet records and records which would reveal the substance of Cabinet deliberations where the public interest in disclosure outweighs the reason for the exception;
e) all cabinet records and records which would reveal the substance of Cabinet deliberations are to be disclosed after 20 years

I would advocate for the same approach in the Northwest Territories, and adopt the Newfoundland definition of “cabinet record”. Furthermore, with the exception of (e) above, (which should remain at the current15 years), I **recommend** that the NWT adopt the provisions of the Newfoundland Act.

3.3 All Canadian jurisdictions include an exemption within their legislation relating to "advice and recommendations" however the types of information identified differ substantially. The current list of information that falls within this discretionary exception has not been reviewed since the Act came into force.

Does the current list of information that is considered to reveal advice remain under this discretionary protection? If no, please indicate what information you would remove, and why.

Section 14 provides for a discretionary exemption from disclosure. As noted earlier, it is my **recommendation** that amendments to the Act make it clear that in the case of all discretionary exemptions, disclosure is the rule and only where there is a demonstrable need to withhold the information should that be done. That is perhaps most particularly true for the application of this section, because much of what goes on in public bodies is the exchange of research, advice, discussions, considerations and options. The potential of this section being used to thwart access to information is real. The onus should clearly be on the public body to provide concrete reasons for non-disclosure. If the exercise of discretion is used to refuse access, there should be a requirement on the public body to provide the Applicant with a detailed explanation for that refusal.

In terms of removing some of the subsections of this section, I **recommend** the removal of (b) - consultations or deliberations involving officers or employees of a public body, a member of the Executive Council, or the staff of a member of the Executive Council. This exemption is far too wide. The words “consultation” and “deliberation” could refer to virtually everything done within a public body, which is not within the spirit or intention of the Act. Everything needed to ensure that public servants can freely and openly give advice is contained in subsection (a). I also **recommend** removal of the words “agency”, “office” and “or other body that is a public body” from subsection (f). Generally speaking, the agendas and minutes of meetings should be open to the public. If the subject matter of the discussion falls within another exemption (for example, personnel issues), that other exemption can be applied. However, any discussion between two employees could, conceivably, be called a “meeting” of an office and this provision used to deny access to records about/surrounding that meeting. That said, most boards, commissions, and corporations make serious policy decisions in meetings so the provision could remain in reference to those sectors of government.

Are there other examples of information that should be included in this section? If yes, please provide examples of records that should be included and why.

There are no additions I would make to this exemption.

3.4 ***All Canadian jurisdictions include an exemption that allows public bodies to refuse disclosure of information considered to be prejudicial to intergovernmental relations. Additionally approvals for decisions relating to this section generally are referred back to the government's executive council.***

A number of jurisdictions also indicate that decision making relating to law enforcement information should be determined by the Attorney General and all other information referred to the Executive Council.

Should decisions regarding access relating to law enforcement information that may affect intergovernmental relations be referred to the Attorney General? If not, why?

This is an issue which, to my knowledge, has not come up during the life of the ATIPP Act. Keeping in mind that

a) all criminal law enforcement in the Northwest Territories is done by the R.C.M.P.,

b) it is unlikely that the possibility of any other kind of “sanction” is likely to affect intergovernmental relations;

I suggest that it may not be appropriate to name the AG to deal with these kinds of issues. I believe that the jurisdictions which have this provision all have local law enforcement agencies.

3.5 ***All Canadian jurisdictions provide a similar exemption within their access and privacy legislation however, the majority of jurisdictions have expanded on the provision "rare, endangered, threatened or vulnerable form of life" as follows:***

> ***"an endangered, threatened, or vulnerable species, subspecies or race of plants, vertebrates or invertebrates; or any other rare or endangered living resources"***

The expanded definition is intended to provide clarification on the different types of species and what should be considered when reviewing the possible application of this provision.

Do you believe the current provision needs to be expanded to include detailed examples as seen in other jurisdictions?

This is, again, not an exemption that is relied on with any frequency. In the 18 years I have been the IPC, it has come up only once in reference to polar bear habitats. As a result, I really have no opinion, one way or another on this issue.

3.6 ***All jurisdictions include a provision that allows public bodies to refuse to disclose information that may harm law enforcement matters. The current list of law enforcement matters within this provision is also similar to other jurisdictions. There are however additional law enforcement information included by other jurisdictions that could be considered for inclusion under this provision:***

- ***reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities,***
- ***reveal information relating to or used in the exercise of prosecutorial discretion,***
- ***adversely affect the detection, investigation, prevention or prosecution of an offence or the security of a center of lawful detention;***
- ***harm the conduct of existing or imminent legal proceedings.***

Is the current listing of law enforcement activities still appropriate in today's environment? If not which activities should be removed and why?

In my opinion, section 20(2)(a) is not in keeping with the spirit and intention of the Act and I **recommend** that it be deleted. This section allows a public body the discretion to refuse to disclose a record where the information “is in a law enforcement record and the disclosure could reasonably be expected to expose to civil liability the author of the record or an individual who has been quoted or paraphrased in the record”. To date, I have not dealt with any review in which this exemption has been relied on. But beyond that, it seems to me that if someone does something or says something that might be actionable in a civil court, it is not appropriate to be hiding that information. Access to

Information legislation is often the only way for an individual to obtain information which might suggest wrongdoing. It is contrary to the focus of the legislation to allow public bodies to hide information which might expose wrongdoing. I **recommend** that this section be repealed.

Should any of the additional law enforcement activities identified above be included in this provision? If yes, which ones?

With respect to the first two suggestions:

a) information which might reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities;

b) reveal information relating to or used in the exercise of prosecutorial discretion,

unlike most southern jurisdictions, the Northwest Territories' only criminal investigation police service is the R.C.M.P. which does not come under the jurisdiction of the ATIPPA or the Office of the IPC. Similarly, this is one of only a few jurisdictions in which virtually all criminal prosecutions are conducted by federal employees. Quite apart from the fact that I believe these "exceptions" are likely covered in the existing list of exceptions, they do not apply to the Northwest Territories at this time.

With respect to the next two:

c) adversely affect the detection, investigation, prevention or prosecution of an offence or the security of a centre of lawful detention;

d) harm the conduct of existing or imminent legal proceedings

I believe these are adequately covered in the existing provisions.

Are there other law enforcement activities that should be considered for inclusion in this provision?

This is not an exception that gets raised frequently. In my opinion, the current list of exceptions are broad enough to cover all of the appropriate exceptions.

3.7 ***The majority of Canadian jurisdictions have expanded this provision to provide public bodies with discretion to refuse to disclose information that may interfere with public safety. This has been generally defined to mean information where the disclosure could reasonably be expected to hamper or block the functioning of organizations and structures that ensure the safety and well-being of the public at large.***

Some jurisdictions have further indicated that information relating to a significant harm to an individual, the public, an affected group, or the applicant must be disclosed, regardless of whether an access to information request has taken place.

Should this provision be expanded to address the broader public safety aspects described above? If no, please explain why?

Nothing in my experience to date suggests that the "safety" provisions should be expanded to include a broader public safety focus. To my knowledge, no situation has arisen in which this has been an issue in the 18 years since the Act came into effect. For that matter, no situation has arisen in which section 21 has been relied on in a review. I can envision a situation in which, perhaps, information **should** be disclosed in the interests of public safety (for example, in the event of a pandemic for the purposes of controlling the outbreak) but those situations would most likely fall under the *Health Information Act*. I have a harder time envisioning a situation in which information being requested under an ATIPP request should be withheld to address public safety issues. I would suggest that most public safety concerns would be covered under one or more of the "law enforcement" exceptions. I'm not convinced, without more, that it is necessary to add these new exceptions.

3.8 ***A few jurisdictions have included a provision that permits public bodies to refuse disclosure of personal information of participants in a formal employee evaluation process. The employee evaluation process is typically known as a "360 degree" evaluation where a peer, subordinate or client of the applicant provides evaluative comments.***

This provision would permit public bodies to withhold the names and positions of subordinates or colleagues, or the identity of students or clients of the applicant. The provision only applies if the information is provided by a participant in a formal employee evaluation process concerning the applicant; it was provided, explicitly or implicitly, in confidence; and the information is personal information relating to the individual providing the evaluation and could reasonably identify the participant

Should this exception be expanded to include a provision that would permit public bodies to withhold the names and positions of subordinates or colleagues, or the identity of students or clients, who provided evaluation information as part of a 360 degree evaluation? If no please explain why?

On the one hand, you want to ensure that people in subordinate situations are confident that there will be no repercussions as a result of a negative evaluation, and on the other hand, the individual the information is about has the right to know what has been said about him/her and by whom, particularly where that information might affect his/her livelihood. The Act currently deals with this by including under the definition of "personal

information" opinions about the individual so that the opinion itself is subject to disclosure but the name of the person who voiced the opinion would be protected as that person's own personal information, the disclosure of which would be an unreasonable invasion of privacy (in most cases). I'm not sure, therefore, if adding another provision to this effect is necessary.

3.9 SCOGO: supports the disclosure of salary information (for GNWT employees), however the current provisions of the Act indicate this would be an unreasonable invasion of a third party's privacy.

All jurisdictions include in their legislation, exceptions relating to the protection of third party personal information. Some jurisdictions have expanded their examples of personal information, which if disclosed would be considered an unreasonable invasion of privacy, to include ethnic origin, sexual orientation and political beliefs or associations.

Other examples of personal information, considered not to be an unreasonable invasion of third parties privacy if disclosed, include remuneration of employees of public bodies. Some jurisdictions that have included this provision indicate that this disclosure insures transparency and accountability for public funds.

Another area of concern raised in relation to the personal information of third parties is the application of the privacy provisions for deceased individuals. Currently, the privacy protections of Section 23 apply whether an individual is alive or deceased. However some jurisdictions have determined that the privacy interests of a deceased individual is considered to decrease over time and a disclosure after a set time period may not be considered an unreasonable invasion of privacy. Time limits reviewed range between 20-25 years before a disclosure may be considered.

However other jurisdictions have raised concerns about a specific cut-off date being used. While the length of time since death is a consideration to be reviewed, a specific cut-off date is not considered the proper measure on how disclosures should be considered. Instead, public bodies should focus on whether the disclosure of information would be an unreasonable invasion of that individual's privacy.

Should the examples of personal information, which if disclosed are considered to be an unreasonable invasion of privacy, include ethnic origin, sexual orientation and political beliefs?

Yes. These are all parts of our personal make-up and identity. Any sexual orientation other than heterosexuality still attracts bigotry and prejudice and many individuals choose to hide their sexual orientation for this reason. While we may not think that this should be necessary, it is a decision for the individual to make, not a public body. In fact, I **recommend** that "sexual orientation" be added to section (23)(2)(j).

While perhaps less obvious, it should also be the individual who decides whether or not to reveal his/her political beliefs. These, too, can lead to discrimination and repercussions. The same holds true for ethnicity. In some people, all of these things may be obvious from they way the look, the way they act or what they say to others. In

those cases, disclosure would not amount to an unreasonable invasion of that person's privacy. Where, however, an individual chooses to withhold that information from the world, that should be their right.

Are there other examples that should be considered?

In light of the rapidly expanding use of biometric technologies, I **recommend** that section 23(2) be amended to include

> where the personal information consists of biometric information about an individual

I also **recommend** that section 23(2)(h) either be deleted or, alternatively, that new wording be found which would narrow the scope of the presumption. As currently worded, the presumption of an unreasonable invasion of privacy applies any time an individual's name appears with any other information about them - what they said, what they did, who they talked to, that they were present in a room at a particular time, that they know another individual....the list goes on. While some of these things, in context, might lead to a conclusion that the disclosure would amount to an unreasonable invasion of privacy, it really does depend on the circumstances and context of the record. This subsection simply spreads the presumption too widely.

Should the examples of personal information, which if disclosed are not considered to be an unreasonable invasion of privacy, include the remuneration of public servants? If not why?

Most jurisdictions are now pro-actively disclosing the remuneration of senior public employees - those who make more than a certain benchmark amount - in annual "sunshine" lists. This benchmark varies from jurisdiction to jurisdiction from approximately $90,000 to about $105,000. This comes as a result of increasing demand from the public to know how public funds are being expended. I **recommend** that amendments be made to the Act which would allow for this. In doing this, you may wish to consider what to include in the calculation of "remuneration" - base salaries? base salaries and overtime? total salaries (including overtime)? benefits? total salaries and bonuses?

I also **recommend** that section 23(4)(e) be amended to clarify "discretionary benefits" or at least to include, specifically, bonuses. I further **recommend** including in section 23(4) the total dollar value of severance agreements (not the details of such agreements, but the total dollar value). Both of these have come up as issues over the years.

Do the privacy interests of a deceased individual decrease over time? Or are there other factors that should be considered?

From those reviews which I have conducted involving the protection of the personal information of a deceased person, I would side with those who have concerns about a specific cut-off date being used. I agree that the focus should be on whether or not the disclosure would constitute an unreasonable invasion of the individual's privacy.

On this issue, I also **recommend**, based on reviews done to date, that an amendment be made to section 48 so as to allow the disclosure of personal information to the executor, administrator or trustee of a deceased person's estate, to the spouse or next of kin of a deceased person or to such other person as might be determined necessary for the settling of the deceased person's affairs. While section 52(1) allows that any right conferred on an individual may be exercised by a personal representative (executor, administrator or trustee), this is a fairly narrowly worded provision. In many cases an estate is not large enough to require a formal application for probate to confirm an executor, administrator or trustee. Furthermore, in the case of a death of an employee, it will often be necessary to gather information about the individual (i.e. income, pension, benefits etc) before a will is probated and a legal personal representative formally named.

3.10 SCOGO: The GNWT should clarify the meaning of the term "prescribed corporation or board" as noted in Section 24(1)f.

Public bodies considering disclosures under this section must balance the public's expectation that they can access information relating to the business of government, against the protections the section provides for third party business interests. All jurisdictions provide a mandatory protection relating to third party businesses.

A number of jurisdictions have expanded this section to include a provision

Is the current list of business information protected under this mandatory exception still appropriate? If no, please indicate what information you would remove, and why.

Section 24(1) needs some work to bring it into line with the way in which business interests are protected in most other jurisdictions in Canada. In most other jurisdictions, the legislation outlines a clear three part test to determine whether third party business information is protected from disclosure:

(a) would the disclosure reveal trade secrets, commercial, financial, labour relations, scientific or technical information of a third party,

(b) was the information supplied, explicitly or implicitly, in confidence, and

(c) would the disclosure reasonably be expected to

(i) harm significantly the competitive position or interfere significantly with the negotiating position of the third party,
(ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied, or
(iii) result in undue financial loss or gain to any person or organization.

Our legislation, as currently drafted, does not require a three part test for any of business information categories. Instead:

- section 24(1)(a) prohibits the disclosure of information that would reveal trade secrets - full stop (a one part test)

- section 24(1)(b) prohibits the disclosure of financial, commercial, scientific, technical or labour relations information (part one of the test) that has been obtained in confidence from a third party or be of a confidential nature and obtained from a third party in compliance with a lawful requirement (part two of the test)

- section 24(1)(c) prohibits the disclosure of ANY information which might result in undue financial loss or gain to any person, prejudice the competitive position of a third party, interfere with contractual or other negotiations of a third party, or result in similar information not being supplied to a public body (a one part test)

I **recommend** the approach adopted by Alberta, Ontario, Newfoundland and others, which requires that the three part test be applied before the prohibition from disclosure which this section affords. This approach is more in keeping with most other jurisdictions and the trend, generally, toward more openness in contracting and procurement matters. In particular, I would refer you to Alberta's FOIPP Act, Section 16, which reads as follows:

16(1) The head of a public body must refuse to disclose to an applicant information

(a) that would reveal
(i) trade secrets of a third party, or
(ii) commercial, financial, labour relations, scientific or technical information of a third party,

(b) that is supplied, explicitly or implicitly, in confidence, and

(c) the disclosure of which could reasonably be expected to

(i) harm significantly the competitive position or interfere significantly with the negotiating position of the third party,
(ii) result in similar information no longer being supplied to the public body when it is in the public interest that similar information continue to be supplied,
(iii) result in undue financial loss or gain to any person or organization, or
(iv) reveal information supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a labour relations dispute.

(2) The head of a public body must refuse to disclose to an applicant information about a third party that was collected on a tax return or collected for the purpose of determining tax liability or collecting a tax.

(3) Subsections (1) and (2) do not apply if

(a) the third party consents to the disclosure,
(b) an enactment of Alberta or Canada authorizes or requires the information to be disclosed,

Further, I **recommend** that this provision be clarified insofar as what is meant by "prejudice to the competitive position of a third party" and "interference with contractual or other negotiations of a third party". These are issues that are often raised by third party companies seeking to protect contract numbers, not only in the Northwest Territories but across the country. As a result, there have been many orders and recommendations made across the country dealing with this issue. A good summary of what would qualify for this exemption law was laid out in a 2013 Order made by the Information and Privacy Commissioner's Office of British Columbia, in *City of Abbotsford* (Order F13-20:

> It is clear that the disclosure of existing contract pricing and related terms that may result in the heightening of competition for future contracts is not a significant harm or an interference with competitive or negotiating positions. Having to price services competitively is not a circumstance of unfairness or undue financial loss or gain; rather it is an inherent part of the bidding and contract negotiation process. (pg. 10)

I **recommend** a provision be added to the Act which makes it clear that section 24(1)(c) does not apply to "pricing and related information in existing contracts".

Should this provision be expanded to protect information supplied to arbitrators, mediator, labour relations officers, or others relating to a labour dispute? If no, please explain why.

The Alberta legislation referred to above does include this as one of the criteria which would qualify the information in question for a mandatory exemption in the third part of the test. I would have no objections to including this expansion of section 24 to include this kind of information, provided that it follows the Alberta model set out above.

Should the term "prescribed corporation or board" be clarified in the legislation?

Nowhere in the legislation or in the regulations is there a definition provided for the term "prescribed corporation or board" in section 24(f). As a result, both 24(1)(f) and (g) currently have no real meaning. If it was intended to apply to public lending corporations, then this absolutely needs to be set out in regulations.

Quite apart from defining what a "prescribed corporation or board" is, I **recommend** the repeal of section 24(1)(f). A business receiving loans from a public lender should still have to establish, under section 24(1) that the disclosure of the information would result in a harm to the business as outlined in the Act.

3.11 All jurisdictions have a similar provision however only the NWT and Nunavut indicate time frames of 6 months. All other time frames range between 30-90 days

Do you have concerns with shortening the time frame under this section? If yes, please explain why. If you do not have concerns with a shorter time frame, what do you consider reasonable?

I have said in many of my review reports that, like justice, access delayed is access denied. A six month delay can be an impossibly long time for anyone on a deadline. In today's digital electronic world, I find it hard to think of a situation in which a public body would be justified in refusing to disclose a record (if it is available) even if it is "required" to be published within a stated time period. As an example, in the case of procurement information, contracts awarded are reported publicly once a year. But someone who has an interest in that information should not have to wait for six months or more to be able to have information about a particular tender award. I **recommend** the removal this exception altogether, but a second alternative would be to reduce the time frame to no more than 30 days.

3.12.1 Currently, public bodies that receive access to information requests relating to workplace investigations must undertake third party consultations with complainants, respondents and witnesses. This results in delays in the release of information. Additionally a number of provisions under Section 23 may require that certain types of information within an investigation report be denied.

A new provision, specific to workplace investigations, could permit public bodies to

disclose to applicants, who are part of that investigation (complainant, respondent) all relevant information created or gathered without conducting a third party consultation

Do you believe including this type of provision in the ATIPP Act would be beneficial to applicants? If no, please explain.

A large number of access requests for personal information about the applicant arise out of some kind of workplace dispute. Individuals who have made complaints against a co-worker or who are the subject of a workplace complaint often request access to all of the information related to the complaint. These are difficult requests to process because they all involve some degree of third party personal information and it is often difficult to give the Applicant the information he/she needs and should be able to access while at the same time protecting the personal information of other parties involved. It is often a delicate exercise to review these records and come up with consistent and predictive results. Often times, when the Applicant is the subject of a workplace complaint, they end up with only a partial picture of how the issue arose and how the matter was handled internally. These kinds of requests also tend to generate large numbers of responsive records and it takes a lot of time to review them page by page, line by line, word by word for the purposes of applying mandatory and discretionary exemptions. This often results in delays in providing the requested records. The proposal outlined in the consultation document seems to me to be a good compromise. It would allow access to all relevant records without having to vet them as carefully for third party personal information. It would avoid the necessity of undertaking third party consultations in some circumstances. And it would limit access to the information to the parties involved and to the extent that their interest lies. This approach would undoubtedly reduce not only the time and effort to respond to access to information requests surrounding workplace disputes, but would reduce fairly dramatically the number of reviews requested of my office. I **recommend** an amendment which would allow disclosure to a complainant or a respondent in a workplace investigation, such disclosure to be without edits (except for the personal information of unrelated third parties) or third party consultations. I am somewhat concerned about prohibiting all other access to such records, for a number of reasons. I **recommend** that for any other person seeking access to these records, they go through the full access process, and that they be accessible subject to any applicable exemptions. In some cases, there is a greater public interest in the outcome of a workplace dispute and those records should, subject to applicable exemptions, be available to the public. Furthermore, the records outlining the outcome of workplace dispute investigations should be available for their precedential value to anyone who seeks the information. There should be some requirement that these records be drafted in such a way as to avoid the use of names and detailed specifics as a measure of protection against breach of privacy when they are made public. There might also be a time period in which these kinds of records are not available to the public, again as a measure to help protect against a breach of privacy.

3.12.1 Currently, exceptions to access identified under our legislation do not provide for any public interest overrides in relation to discretionary exceptions

Should the Act be revised to provide a public interest override in relation to specific discretionary exceptions? If yes, which specific discretionary exception should include this?

Our current legislation does, in fact, have a couple of provisions which amount to a public interest over-ride. The first is in section 23(3) which outlines some of the circumstances which should be considered by a public body when evaluating whether or not the disclosure of personal information would amount to an unreasonable invasion of privacy. This section provides that some of the circumstances to be considered include:

a) whether the disclosure is desirable for the purpose of subjecting a public body to public scrutiny;
b) whether the disclosure is likely to promote public health and safety or to promote the protection of the environment; and
c) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people

These are all "public interest" issues which must be considered in determining whether or not the disclosure of personal information is an unreasonable invasion of privacy.

Furthermore, section 48(s) provides that a public body may disclose (or use) personal information:

> for any purpose when, in the opinion of the head,
>
> > (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure,

It is noteworthy that both of these provisions apply only to the disclosure of personal information.

More generally, it has always been my position that disclosure of records is the rule and the only time access should be declined is when there is a good, thoroughly considered reason for the refusal and this is particularly so when the exemption being relied on is a discretionary one. In other words, it is my position that disclosure is the starting point. With this approach, there is no need for a public interest over-ride with respect to discretionary exemptions. My **recommendation** would be an amendment or amendments to the Act which explicitly state that in the case of discretionary exemptions, disclosure is the rule and the reason for a refusal to disclose will have to be accompanied by a full explanation of the criteria used in the exercise of discretion to refuse access.

As noted above, in the case of section 23, a limited public interest over-ride already exists. I would agree that there is merit in considering a public interest over-ride to attach to other discretionary exemptions as well. It should be noted that the Supreme Court of Canada concluded, in the case of *Criminal Lawyers' Association* [2010] SCC 23 which arose out of Ontario, that the law in that jurisdiction requires a public official exercising discretion under the access to information legislation to weigh all relevant considerations for and against disclosure, including private and public interests.

If a public interest override is put forward, which model (Ontario or NFLD) would work best in the NWT?

If we were to use either the Ontario or the Newfoundland model, I would opt for the Newfoundland model which is, in my opinion, clearer and easier to both understand and apply.

4. REVIEWS AND APPEALS

4.1 SCOGO Recommendation: recommends the 30 day appeal period for applicants or third parties wanting to request a review with the IPC be extended.

The majority of NWT time frames relating to the third party consultation process and the review process are, along with Nunavut, the longest time periods in Canada. Concerns relating to the time frames have been raised by applicants.

However the 30 day appeal period for an applicants or third party to request a review with the IPC ranges between 15-60 days.

Should the time frames relating to third party consultations and reviews be shortened? If yes, what do you consider reasonable time periods?

The time frame for the third party consultation period is far too long. By the time the notice to third parties goes out, it is often late in the initial response time frame - 30 days. The notice goes out to the third parties who have 60 days from the time they get the notice to provide their input, bringing us to close to 90 days. The public body then has an additional 30 days to complete the request, bringing us to 120 days. Where the public body decides to disclose the records in question, they must give notice of that intention to the third party and give them yet another 30 days to seek a review from the IPC which means that the Applicant will not be receiving a response to his/her request for information for at least five full months from the date he/she submitted it, at the earliest.

I would suggest that if a third party has a real objection to disclosure, it will be obvious from the minute that the correspondence is received. I **recommend** that the initial response period be reduced to no more than 21 days from receipt of the notice (the consultation period). I would give the public body no more than 10 days after the

consultation period to make a decision on disclosure and allow for between 21 and 30 days for the third party to submit a Request for Review to the IPC. This would reduce the total time for the consultation process from 5 months to about 3 months, which is still longer than many Applicants would like, but is much shorter than the current process.

Should the time frame relating to the 30 day appeal period for applicants and third parties be extended? If yes, what do you consider a reasonable time period?

I would not **recommend** extending the 30 day appeal period for third parties. Rather, I would reduce that time frame to 21 days. In any other circumstance, there should be no time limit for the filing of Requests for Review from the IPC. If there is to be a time limit, I would recommend that the IPC be given the authority to extend the time for filing where such an extension would not result in any prejudice to any person.

4.2.1 Concerns have also received from public bodies and applicants that the process relating to conducting reviews are confusing for all parties.

Are the processes relating to third party consultations and requests for reviews confusing? If yes, should these processes be clarified by amending the Act?

The process relating to third party consultations is somewhat complicated and even a little confusing because the third party has to make its case for non-disclosure first to the public body which may, or may not, accept the objections raised. The third party is then given notice that their information is going to be disclosed notwithstanding any objections raised and, in order to prevent that from happening, the third party has to file a Request for Review. The only way to reduce this confusion, I think, might be to remove the initial consultation with the third party altogether. Instead, where the public body intends to disclose a record which might affect the interests of a third party, give both the Applicant and the third party notice of the decision and of their right to seek a review by the IPC. This is, I think, how the Newfoundland legislation is set up. It would also reduce the response time in situations where there are third parties rather dramatically.

The Request for Review process itself is not, to my mind, overly complicated. It mirrors the process for most parts of the country and does not need any significant changes.

On a related matter, however, it should be noted that in the 18 years since the legislation came into effect, only a very small handful of matters have been appealed to the Supreme Court. One might hope that this is because we do such a good job in the response and review stages that everyone is satisfied with the outcome. That would, however, be naive. One of the main reasons that there are so few appeals to the Supreme Court is that the process of taking that step is complicated and expensive. Furthermore, there are no real “processes” in place to guide an Applicant or the court in terms of how that appeal process should work. For example, there is nothing to suggest

how the cause should be styled, or what the Notice of Appeal should look like, or what should accompany that notice (an affidavit? A copy of the Review Recommendation? A copy of the decision of the head of the public body?). I recently received a letter from a corporate Applicant who wanted to appeal a decision to the Court. He managed to file a Notice of Appeal but quickly withdrew because it became clear that the processes expected by the court were far beyond his abilities and it would have cost too much to hire a lawyer to assist. If that is the case with a corporate Applicant with some financial depth, it is unlikely in the extreme that an individual will have the resources or the ability to appeal to the court. One way to address this would be to change the format of our legislation to provide the IPC with the power to make Orders. That would necessitate some changes to the review process which is currently fairly informal. Without getting into a discussion of the relative merits of order making power v. the ombudsperson model, I simply provide comment that the inability of most people to seek court redress is a barrier to access to information that should be addressed in some way. One option might be to consider the Manitoba model which provides for a specialized adjudicator to make final order.

4.2.2 The NWT time frames relating to a privacy complaint process are, along with Nunavut, the longest time periods in Canada.

Should the time frames relating to third party consultations and reviews related to privacy complaints be shortened? If yes, what do you consider reasonable time periods?

With respect to third party consultations, see my comments with respect to 4.1 above.

With respect to privacy complaints, depending on the work load of my office, the minimum time necessary to complete a review and report is about four months (120 days). The public body is normally given 30 days to explain the circumstances related to the privacy complaint and the complainant another 30 days to respond to the public body's explanation. On occasion, additional time is required to obtain further submissions or comments from either or both of the parties. The review recommendation itself is usually completed within two months after all information has been gathered. This depends largely on the workload in the office at any point in time. Shortening the 180 day period provided to the IPC to complete a review would require, a commensurate increase in manpower in the office of the IPC.

The nature of a review of a privacy complaint is quite different from a review of an access to information matter. While access reviews often require a page by page, paragraph by paragraph review of hundreds, if not thousands of pages of records, privacy reviews are more of a fact finding/policy review exercise. Sometimes they can be completed quite quickly but in some circumstances it takes a fairly long time to determine what happened to lead to the breach. It should be noted that, in terms of the harm done, there is nothing that can be done to "undo" a privacy breach. It has already been committed and the damage to the Complainant, if any, has already been done by

the time the matter reaches the IPC. In the vast majority of cases, shortening the length of time taken to review the incident and address it isn't going to improve the complainant's situation, but it may reduce the thoroughness of the review. In other words, the time frame for dealing with a privacy complaint, unless the breach is ongoing (which is something that has not yet crossed my desk) is less critical.

I would retain the 180 day time period for completing both access and privacy breach reviews. I do, however, believe that the 90 days given to the public body to respond to a privacy breach review should be shortened to 45 days.

5. PROTECTION OF PRIVACY

5.1 ***Currently under this section of ATIPP, approval is required from Executive Council in circumstances where it is necessary to collect personal information in advance of a program or activity being operational. This approval is intended to provide an added protection to individuals whose personal information may be collected before a program's purposes are fully defined or documented. This provision may no longer be required in our current privacy environment.***

The Act does not include a specific provision dealing with the collection of personal information for the purpose of planning or evaluating a program or activity of a public body. Planning and evaluation information from a program is typically not considered information that relates directly to the administration of the program, therefore public bodies are restricted on what they can collect for this purpose. However with the increase in planning and evaluation related activity there may be a need to provide specific authority.

Is the provision requiring public bodies to seek approval from Executive Council for the collection of personal information for a proposed new program or activities still required?

I have only seen section 40(c)(ii) of the Act relied on in one case since coming into effect and that situation arose in Nunavut. In that case, the provision was not used "to provide an added protection to individuals whose personal information may be collected before a program's purposes are fully defined or documented". Rather, it was used to authorize the collection of significant and detailed personal information without consent from the patients for an ongoing health surveillance program which had no legislated mandate. The Minister of Health, in that case, relied on the section of the *Hospital Insurance and Health and Social Services Administration Act* which allows the Minister to conduct surveys and research programs as well as a decision made by the Executive Council to approve the collection and consolidation of health data on a mandatory basis without the requirement of consent for an ongoing health surveillance program. In my opinion, public bodies should not be allowed to collect personal information for a "proposed" program or activity. I **recommend** that this provision either be clarified or repealed.

Should the Act be expanded to allow for the collection of personal information for program evaluation or planning? If no, why not?

I am strongly opposed to the collection of personal information for such purposes. I can think of few, if any, circumstances in which it should be necessary to have identifying information about individuals to either plan future programs or evaluate existing ones. This can be done with statistical or de-identified information. If for some reason there is a real need to collect personal information for these purposes, those purposes should be outlined at the time of collection and the individual should be given the option to opt out of such use. In other words, if a public body is collecting information for the purpose of program evaluation or planning, they know or should know at the time of collection that that is the purpose for the collection and this should be disclosed to the individual.

5.2 ***Currently our legislation does not allow for the collection or disclosure of personal information for the delivery of common or integrated programs. Public bodies are required to create and administer a series of consent forms for the disclosure of information between public bodies, even though it's related to an integrated program intended to benefit the client. This can result in delays in the delivery of services to clients and add to the administrative burden.***

Other Canadian jurisdictions have addressed this issue by including a provision in their legislation that permits the indirect collection and disclosure of personal information if the information is necessary for delivery and evaluation of a common or integrated program or activity.

Other jurisdictions have also included provisions in their legislation that would permit the indirect collection of personal information if the information is used to:

- ***determining suitability for an honour or award, or scholarship, prize or bursary;***
- ***assist with an existing or anticipated proceeding before a court or judicial or quasi-judicial tribunal***

Do you support allowing public bodies to indirectly collect personal information for the purpose of

a. Providing information for Integrated program services;

No. If a public body is planning to collect information for integrated program services, they should be collecting it from the individual and advising them why the information is being collected and how it will be used. At the core of the issue is the right of the individual to determine what and how much personal information will be collected/used and for what purpose. While it may be viewed as more efficient to allow the sharing/collecting of personal information for such programs indirectly, the information does not belong to the GNWT, but to the individual and the individual should be able to decide how that information is used. Consent should be required.

b. Evaluating a common or integrated program or activity;

No. As noted above, there should never be any circumstances in which personal information in identifiable form should be necessary for evaluation purposes. Evaluation can be done without the need to attach personal information to the evaluation data. If for some reason personal information is needed for evaluating a program, such information should be collected only from the individual to whom the information relates and only with knowledgeable consent.

c. Determining suitability for an honour or award, or scholarship, prize or bursary;

In most cases, those who are being considered for an honour, award, scholarship or prize are aware of that fact and should be able to consent to the direct and/or indirect collection of their personal information. This can be done by having the individual sign the nomination/application form. Where the individual is not aware that he/she is being considered for such an honour, award, scholarship, prize or bursary, the current section 41(1)(g)(i) and (ii) are probably sufficient to allow for indirect collection for these purposes.

d. Providing information for proceedings before a court or judicial or quasi-judicial tribunal?

This is already provided for in section 3(2)(c) and (d).

5.3 While it may be obvious that notice would not be required for the collection of information for law enforcement purpose, other jurisdictions have specifically set that out in their legislation.

Is there need for a provision that clearly indicates that the notification requirements do not apply when the personal information is being collected for the purpose of law enforcement?

Section 41(1)(c) as currently written provides that a public body may collect personal information indirectly where the information is collected for the purpose of law enforcement. If information is being collected directly from the individual, and the matter is a law enforcement issue, it seems to me that the individual has a right to know why the information is being collected so that he/she can make a considered decision about whether or not to provide the information requested. Everyone should have the right to avoid “incriminating” themselves.

5.4.1 While all jurisdictions in Canada use PIAs to some degree, the majority of jurisdictions provide for the use of PIAs in government policy or directives, however in some jurisdictions the requirement for a PIA required is set out in their legislation.

Should PIAs be required in legislation or is the use of government policies and/or directives acceptable?

There should be a legislated requirement for PIAs to be completed at the preliminary stages of establishing policies and programs. It is my experience that PIAs are currently the exception, not the rule, when public bodies are considering new programs, procedures, policies and legislation, notwithstanding the existence of a tool created by the ATIPP Office for that purpose. Policies and directives are clearly not ensuring adequate consideration of privacy issues at the right stages of new projects. The earlier in the development process that privacy issues are identified, the more likely it is that they can be dealt with in a substantive and effective way. I **recommend** a legislated requirement that PIAs be conducted for all new projects in which there is any possibility that personal information will be involved. Further, I **recommend** that PIAs be conducted any time there is a possibility that third party contractors will have access to personal information collected or in the possession of a public body. Finally, I **recommend** that any purchase of new technology undergo a review to ensure that it will comply with the privacy and security requirements imposed by the ATIPPA.

5.4.2 The framework relating to privacy breach reporting requirements varies across Canada. Similar to PIA requirements, the majority of jurisdictions provide for it through policies or directives. Currently the GNWT Information Incident Reporting falls under a government directive

Should information incident reporting be required in legislation or is the use of government policies and/or directives acceptable?

Once again, my experience over the course of 18 years as the Information and Privacy Commissioner suggests to me that reporting of "information incidents" is lacking. There have been only a very few incidents which have resulted in a report to my office. While I would like to think that the Government of the Northwest Territories is more effective at preventing breaches and losing track of personal information than other governments, I am fairly sure that there are far more breaches than are either not recognized as breaches, or if recognized as breach, that are not reported. Nunavut and Newfoundland both have added data breach notification requirements to their respective legislation. Other jurisdictions are currently considering such amendments. Our own *Health Privacy Act* and all health privacy legislation in Canada, has breach notification requirements. Information is a valuable commodity and it is important that the public be able to trust that when governments collect personal information, they will be held to a high standard in protecting it from inappropriate loss or disclosure. The

best way to do this is to require public bodies to report incidents. I **recommend** a breach notification section be added to the ATIPP Act, if only to keep it current with the direction that legislation across Canada is taking generally.

5.5 A number of other Canadian jurisdictions permit their post-secondary educational bodies to use personal information from their alumni records for the purpose of fund raising activities specific to the education body. However post-secondary educational bodies must discontinue using this information when requested to do so by the individual to whom it pertains.

Do you have any concern with permitting NWT post-secondary educational bodies to use the personal information from their alumni records for fundraising? If no, why?

Yes, I have significant concerns. Individuals who seek post secondary schooling in the Northwest Territories have no option but to provide significant personal information to the institution. Their intention in providing such information is to obtain a higher education, not to be solicited for contributions. Just as hospital foundations are not allowed to use patient information for the purpose of fundraising, post secondary institutions should not be able to use student information for that purpose. There is nothing to stop a post secondary institution from obtaining explicit consent to this use their student's personal information during their student days. If consent is not obtained, the information should be out of bounds.

5.6 Disclosures under this section may only occur in the specific circumstances outlined in the legislation. If the disclosure is not identified, public bodies cannot disclose the information.

A jurisdictional review of disclosures of personal information has identified both new and expanded provisions. The expanded provisions are intended to provide greater clarity relating to the permitted disclosure and to permit disclosure in areas that had not been previously anticipated. Examples of expanded provisions are noted below:

- ***Section 48(e) - to a public body or a law enforcement body for law enforcement purposes:***
  - ***where the public body is a law enforcement agency and the information is disclosed to another law enforcement agency in Canada of a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.***

- ***Section 48(k) to an officer or employee of a public body or to a member of the Executive Council, if the information is necessary for the performance of their duties.***
  - ***Or for the protection of the health or safety of the officer, employee or minister***

- ***Section 48(q) when necessary to protect the mental or physical health or safety of any individual.***

- ***where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is given in the form appropriate in the circumstances to the individual the information is about.***

- ***Section 48(r) so that the next of kin or a friend of an injured, ill, or deceased individual may be contacted.***
  - ***So that a spouse or adult interdependent partner, relative or friend of an injured, ill or deceased individual may be contacted.***

- ***Section 48(t) when that information is available to the public***
  - ***If the personal information is information of a type routinely disclosed in a business or professional contact and the disclosure***
    - ***i) is limited to an individuals' name and business contact information(title, address, phone and fax number, email and does not reveal any other personal information about the individual)***

New Provisions for Consideration

- ***To an officer or employee of a public body or to an member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed (previously discussed in section 5.2);***

- ***To a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry;***

- ***To the surviving spouse or relative of a deceased individual where in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased' personal privacy;***

- ***For the purpose of i)licensing or registration of motor vehicles or drives, or ii) verification of motor vehicle insurance, motor vehicle registration or drivers licenses.***

- ***For the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside of Canada by government bodies of professions and occupations;***

- ***Of information i) disclosed on a social media site by the individual the information is about, ii) was obtained or compiled by the public body for the purpose of enabling the public body to engage individuals in public discussion or promotion respecting proposed or existing initiatives, policies, proposals, program or activities of the public body or respecting legislation relating to the public body, and iii) is disclosed for a use that is consistent with the purposes described in ii).***

Is there a need to expand our current provisions (noted above) for greater clarity or understanding?

Section 48(e) - to a public body or a law enforcement body for law enforcement purposes:

- where the public body is a law enforcement agency and the information is disclosed to another law enforcement agency in Canada or a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority.

While I applaud any provision which would limit the ways in which personal information can be used/disclosed (and I think this change would narrow the circumstances in which this section would apply) I have concerns about exactly how this would work in light of the definition of "law enforcement". Currently, that definition includes not only policing, but also investigations or proceedings that lead or could lead to the imposition of penalty or sanction. This is a very wide definition that includes a range of other "law enforcement" activities, as, for example, discipline bodies in various professions and industries. Before making this amendment, some consideration should be given to how it's application would play out.

Section 48(k) to an officer or employee of a public body or to a member of the Executive Council, if the information is necessary for the performance of their duties.

- Or for the protection of the health or safety of the officer, employee or minister

This amendment is unnecessary in light of the fact that section 48(q) allows for a disclosure of personal information "when necessary to protect the mental or physical health of any individual".

Section 48(q) when necessary to protect the mental or physical health or safety of any individual.

- where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is given in the form appropriate in the circumstances to the individual the information is about.

I would support this clarification of this subsection.

Section 48(r) so that the next of kin or a friend of an injured, ill, or deceased individual may be contacted.

- So that a spouse or adult interdependent partner, relative or friend of an injured, ill or deceased individual may be contacted.

I would support this clarification of this subsection.

Section 48(t) when that information is available to the public

- If the personal information is information of a type routinely disclosed in a business or professional contact and the disclosure
  - is limited to an individuals' name and business contact information(title, address, phone and fax number, email and does not reveal any other personal information about the individual)

I would support this clarification.

To an officer or employee of a public body or to an member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed (previously discussed in section 5.2);

See my comments above on this issue. I would not support this amendment to the Act.

To a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry.

There is no need for such an amendment. Any authorization in writing from the individual to use/disclose his or her personal information is effective to authorize that use/disclosure.

To the surviving spouse or relative of a deceased individual where in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy.

There should be some provision which allows a public body to disclose limited information about a deceased person to someone authorized to receive it, such as an executor or trustee, or in the absence of an executor or trustee, a spouse (being careful how we define this word) or next of kin (see discussion below).

For the purpose of

i) licensing or registration of motor vehicles or drivers, or
ii) verification of motor vehicle insurance, motor vehicle registration or drivers licenses

I cannot think of any situation in which personal information would need to be disclosed to a third party for the licensing or registration of motor vehicles or drivers, unless the disclosure is to a third party contractor who actually prints the licenses. I would think that 48(a) would cover this kind of disclosure (disclosure for the purpose for which the information was collected). In terms of verification of insurance, motor vehicle registration or drivers licences, I think this is probably included in the legislation of other

jurisdictions because their police forces are provincial or city run institutions. That is not the case here. This use or disclosure would fall under a number of other allowable disclosures - 48(a), (e), and likely (u). An amendment such as this one is, in my opinion, not necessary in the Northwest Territories.

For the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside of Canada by government bodies of professions and occupations.

There is some merit in this sort of amendment, although, as noted above, discipline of persons in regulated industries would, under our Act, be considered a "law enforcement" matter and section 48(e) would apply. If there were to be a change to the definition of "law enforcement", this kind of provision should definitely be included.

Of information

i) disclosed on a social media site by the individual the information is about,
ii) was obtained or compiled by the public body for the purpose of enabling the public body to engage individuals in public discussion or promotion respecting proposed or existing initiatives, policies, proposals, program or activities of the public body or respecting legislation relating to the public body, and
iii) is disclosed for a use that is consistent with the purposes described in ii).

I am strongly opposed to such an amendment. Much of the public still fails to understand the reach of social media or appreciate the consequences of comments made on a social media site. If a public body wants to "engage individuals in public discussion", those individuals should be explicitly advised when the comments are collected they might be further used or disclosed.

5.7 ***The majority of jurisdictions include provisions for disclosures of personal information for research purposes in their access and privacy legislation. Similar to the NWT, the provision includes conditions relating to the security and confidentiality of the information.***

However a number of jurisdictions also include a provision that permits their government Archives to disclose personal information for archival or historical purposes, if the disclosure is for historical research and would not be considered an unreasonable invasion of a third party's privacy. If the requested research involves deceased individuals, the research may only be considered for individuals who have been deceased for 20 years or more or the information itself has existed for over fifty years.

Is there a need to expand the disclosure of personal information for research purposes to include disclosures for historical research through the NWT Archives?

I have no sense of how much historical research is done through the NWT Archives or whether the Archives are treated any differently, in terms of privacy, than other public records. I note that not all records in the Archive are "owned" by the GNWT and, in fact, section 3(1)(e) explicitly states that the ATIPP Act does not apply to records placed in the NWT Archives by or for a person other than a public body. That said, personal information does not change in character when it leaves the GNWT and is placed in the archives. If personal information is going to be disclosed by the archives, I would suggest that it should need to meet the same tests for disclosure as any other record in the possession and/or control of the GNWT. There are provisions for research generally and I would suggest that these provisions would apply as well to records in the archives.

If yes, should there be similar conditions relating to deceased individuals or the existence of information over 50 years old?

Are there other research considerations that should be included in this section?

6. INFORMATION AND PRIVACY COMMISSIONER

6.1 Currently, under the Act an IPC may serve for five years or until they are reappointed or a successor appointed. There is no limit on the number of terms that an IPC can serve. Appointments for IPCs in Canada typically range between 5-7 years. However the federal government and five other provinces and territories have restricted the IPC's term of office to either one term only (New Brunswick) or two successive terms, (Yukon, Newfoundland, New Brunswick, Manitoba and Saskatchewan).

Should the number of terms in office that one NWT Information and Privacy Commissioner can hold be restricted? If yes, what should be the maximum length of term and how many terms should the IPC be allowed to serve?

Any comments I make in response to this question should be taken in the context they are given. I have served as the part-time IPC for some 18 years and am confident that the Northwest Territories is well served by the work I do. There is much to be said for consistency and continuity, particularly in a complicated area of practice such as this where expertise is limited. This is even more so where there are no other expert area staff in the office who could afford corporate knowledge and continuity. That said, change can be a good thing and at some point is necessary. The Legislative Assembly has the option not to reappoint an IPC every 5 years if they so choose. The five year term is, in my opinion, an appropriate length of time for each term of office. Until such time as there is a deeper pool of expertise in the area of access and privacy within the Northwest Territories, however, I would not recommend limiting the number of terms an IPC can serve.

6.2 ***Concerns were raised in the media that the ATIPP Act provides no real transparency and the IPC power to make recommendations is not sufficient and she needs greater power. It appeared the media was referring to the need for order making powers.***

The IPC has previously noted there are pros and cons for both models, but of the two she preferred the ombudsperson model as it provided the ability to meet the spirit and the intention of the Act in a more collegial way.

Recently however the IPC has raised concerns about the costs and complexity applicants face who wish to appeal a matter to the NWT Supreme Court. In light of these concerns she has noted that while full order making powers may not be necessary, some changes in her powers may be necessary to address this concern.

Should the Act be revised to provide the NWT IPC with order making powers? Are there other ways of addressing the issues raised by the IPC?

As noted in the discussion paper, I have commented on this issue a number of times over the years.

The benefits of an "ombuds-model" for the office of the IPC include:

- the process is less formal and, therefore, can be completed much more quickly;
- there is more room to make suggestions for change which may fall outside of what can/should be ordered. For example, when it comes to a privacy complaint, the IPC can make expansive suggestions for changes to policies and procedures and recommend that those changes be made throughout several departments. If making orders, the orders would have to be far more focussed;
- the process is not adversarial

There are drawbacks to this system that would at least partially be addressed by an "order making" model:

- the lack of order making power encourages a lack of respect for both the office of the IPC and the ATIPP Act itself. In one of the very few applications under the Act to the court in the Northwest Territories, *CBC v. Northwest Territories (Commissioner)* 1999 CanLII 6806 (NWTSC), Justice Vertes made the following comments at paragraphs 16 and 17:

> The purposes of the Act, as recited above in s.1, are to make public bodies more accountable to the public and to protect personal privacy by, among other things, providing for an independent review of decisions made under the Act. Presumably that is a reference to the Commissioner. Yet the Commissioner, while empowered to review, can only make recommendations. The government is free to ignore those recommendations. The head of

> the public body may make any other decision the head considers appropriate : s.36(a). So, could it be that the legislature intended to create a position that performs inconsequential functions (irrespective of the expertise that the Commissioner may develop in analyzing and applying the Act)? I think a broader question to ask is whether an independent review can be at all meaningful if there is no enforcement power or where the results of that review bind no one.
>
> Based on my analysis of the role of the Commissioner, and the fact that it is the department head's decision that is the focus of the appeal, the recommendations and report of the Commissioner, insofar as they were adopted by the head, are entitled to little or no deference.

This attitude is toward the office, though perhaps surprising in light of the fact that there are many IPCs in Canada who have only the authority to make recommendation, is not unique. There are more than a few who see the lack of order making authority in the IPC as limiting the respect to be afforded to the office.

- public bodies often provide only cursory and incomplete submissions to the IPC in responding to the review process and in meeting their onus under the Act to establish, for example, when an exemption applies. If the public body knew that a failure to respond completely and thoroughly would result in an enforceable order against them, they would be more likely to provide more thorough explanations, which will lead to more consistency, and a better understanding of the Act overall;

- the onus will be on the public body (rather than on the Applicant) to bring a matter to court if they disagree with the Order made. Public bodies are in a much better position to do this than most applicants.

The "order making" model would certainly require additional staff in the office of the IPC to address the more formal approach to inquiries and to allow mediation attempts between the parties without the participation of the IPC him/herself.

If Order making power were to be considered, I would suggest that there may be some merit in applying it only to Requests for Review with respect to Access to Information matters. Access to Information deals with physical records and whether or not they should be disclosed and this is more conducive to the making of an order. Privacy complaints, on the other hand, are received after the damage has already been done and, in most cases, the only thing that can be done on review is to make recommendations (or orders) with respect to changes in policies or procedures or legislation. To limit the IPC's authority to "order making" power in the case of privacy

concerns would be to reduce the focus of the IPC's reports to the very narrow complaint and limit her ability to influence policy and approaches on a larger scale.

As you know, Newfoundland and Labrador have recently passed legislation which imposes what they call a "hybrid" model. The IPC still makes recommendations only. The difference is in how a public body responds to the recommendations. Public bodies now have two choices: they can accept the recommendations made, or they can apply to the court for a declaration that, by law, the public body is not required to comply with the recommendation. This model holds some attraction for me as the IPC, in particular because it maintains the efficiency and informality of the ombuds-model while shifting the onus of an appeal to the public body which is far better placed to undertake such an endeavour. Keeping in mind that approximately 90% of recommendations are accepted by public bodies, the extra burden on public bodies would not be that significant, particularly if it also results in better submissions to the IPC in the first place.

Another option would be to give the IPC the authority to appeal decisions of public bodies to the courts on behalf of Applicants. Knowing that this is possible might encourage public bodies to be more thorough in their initial submissions to the IPC. It would also make public bodies pay closer attention to the recommendations made and take a more purposeful approach to their decisions. It would simply give the IPC that extra measure of authority which would make public bodies a little more careful in dealing with him/her.

Yet another option would be to follow the model in Manitoba which allows an applicant the ability to "appeal" the decision of the head of a public body to an Adjudicator, appointed by the Legislative Assembly for that purpose, with the decisions of that person to be final.

Either way, I **recommend** that the IPC be given order making power with respect to administrative matters, such as the application of fees, extensions of time and the authority to disregard a Request for Information.

6.3 ***Currently, the IPC's review powers do not provide for mediation between public bodies and applicants. In Newfoundland, their legislation allows the IPC to take the steps necessary to attempt to resolve a request for review regarding access to information or a privacy complaint informally, to the satisfaction of the parties.***

The Newfoundland legislation sets a time limit of 30 business days for the mediation. If the matter is unable to be resolved informally, the IPC may then undertake a formal review of the matter.

The IPC has recently raised concerns that the current privacy complaint process only allows her to undertake a review when a formal complaint has been received by her office. The IPC commented that a number of privacy issues have been brought to her attention; either through the media or by individuals who are unwilling to file formal complaints. In these circumstances she is not able to initiate a privacy review into the matter.

Should the Act be revised to permit the IPC to attempt to mediate access to information requests or privacy complaints??

It is to be noted that I often attempt to undertake an informal mediation with respect to Requests for Review which come to my office. It may be of some benefit to include a specific provision in the Act which would allow for a more formal approach to mediation so as to encourage both applicants and public bodies to suggest or consider a mediation. This would work particularly well with respect to privacy complaints. The concern I would have with respect to a more formal mediation program is that this would require more resources within the office of the IPC. It would be difficult for the IPC to undertake a formal mediation and then move on to completing a review report while maintaining the appearance of impartiality. The IPC would have to either engage someone outside her office to undertake mediations or hire an employee who has mediation training and skills.

Should the Act be revised to permit the IPC to initiate a privacy review even though a formal complaint has not been made?

There have been a number of instances in which I have become aware of serious privacy issues within public bodies but have been unable to do a formal review because the Act currently does not allow for the IPC to initiate a review without first receiving a formal complaint. Often times, complainants are reluctant to come forward to make a complaint because of fear of reprisals of one form or another. I would fully support and **recommend** that the IPC be given authority to initiate privacy reviews without a formal request in appropriate circumstances.

6.4 The IPC's general powers are specific to those identified above, however several jurisdictions have expanded the IPC's "general powers" to include;

- ***providing educational programs to inform the public about the Act and their rights***
- ***the authority to consult with any person with experience or expertise in any matter related to the purpose of this Act;***
- ***providing comments on the privacy implications relating to the use of information technology in the collection, storage, use or transfer of personal information;***
- ***taking action to identify and promote adjustments to practices and procedures that will improve public access to information and protection of personal information;***
- ***bringing to the attention of the head of a public body a failure to fulfil the duty to assist applicants;***
- ***inform the public from time to time of apparent deficiencies in the system, including the office of the IPC.***

Should the general powers of the IPC be expanded to include any of the powers noted above? If yes, please identify which ones and why?

I **recommend** the addition of all of the new “general powers” identified in this section of the discussion paper. In my role as IPC over the years I have undertaken all of these activities from time to time and I would argue that at least some of them are implied in the wording of various sections of the current Act. That said, as the IPC’s jurisdiction to

act arises exclusively from the Act, adding these as explicit powers will ensure that when these powers are used and activities undertaken, there can be no question as to the IPC's jurisdiction.

7. GENERAL AND OTHER MATTERS

7.1 Other situations to consider regarding the exercising of rights by other persons are:

- ***If someone is acting as an agent as designated under the Personal Directives Act. In that case they may exercise that individual's rights in relation to the powers and duties given to the agent under the personal directive.***
- ***If someone is acting under the authority of a power of attorney. A power of attorney is an authority given to one person (called the attorney) to do certain acts in the name of, and personally representing, the person granting the power (called the donor).***

Should the Act be amended to include the exercise of rights by other persons as set out in a personal directive or a power of attorney? If no, please explain why.

Neither the *Powers of Attorney Act,* nor the *Personal Directives Act* were in existence when the *Access to Information and Protection of Privacy Act* came into effect. That said, Section 52(1)(d) already provides for the disclosure of personal information to someone who has been granted a power of attorney "if the exercise of the right or power of attorney relates to the powers and duties of the attorney conferred by the power of attorney". This section should perhaps be amended to make reference to a "power of attorney validly made by a donor in accordance with the *Powers of Attorney Act".*

Section 52(1)(e) also provides that personal information can be disclosed to "any person with written authorization from the individual to act on the individual's behalf". This would, I think, include a personal directive under the *Personal Directives Act.* However, once again, perhaps section 52 should be amended to include reference to a personal directive validly executed by an individual, provided that the specifics of the personal directive relate to the information being requested/imparted.

Are there other situations where someone else may need to act for an applicant that should be considered?

I can think of none.

7.2 Newfoundland's legislation includes a provision that provides no action lies against Members of their Legislative Assembly for disclosing information obtained from a public body in instances where they are acting on behalf of an individual they are assisting with a problem. (Section 48(v).

Should protection from liability be expanded to include protection for Members of the Legislative Assembly when acting in accordance with the section above?

By definition, the term "public body" currently excludes the Legislative Assembly and members of the Legislative Assembly. The result is that if a Member of the Legislative Assembly discloses the personal information of a constituent or another person they are assisting with a problem, there are no consequences, at least under the provisions of the Act. In my opinion, rather than providing that MLAs be protected from liability under the Act, I would instead **recommend** that the Act be amended so as to provide that MLAs are subject to the privacy provisions of the Act and can be liable for disclosing personal information except in accordance with the Act (which, in most cases, will mean obtaining the individual's express consent to the disclosure and the specifics of the disclosure).

7.3 Other jurisdictions have included the following activities as offences:

- ***If someone destroys records that are subject to the Act, or directs someone else to destroy records for the purpose of evading a request for access to the records,***

- ***If someone either attempts to gain access or in fact gains access to personal information under which they have no authority to do so.***

Fines in relation to these offences generally range between $1,000 to $10,000.

Should the Act be revised to include either of the two activities noted above? Are there other offences or penalties that should be considered?

Absolutely yes.

In addition, I strongly **recommend** that a new Part be added to the Act which provides for a clear "duty to document" and that there be a consequent amendment to the offences section to provide that it is an offence to fail to properly document the work of government employees and agents. Appropriate file management and failure to adequately document decisions made by government and government agencies is becoming a serious and significant issue across the country. The BC Information and Privacy Commissioner recently issued a detailed report outlining some of the issues being dealt with in British Columbia surrounding the failure to properly document (and the improper destruction) of important working records in certain B.C. government departments. Her conclusion:

> Government is well advised to introduce a legislated duty to document its key actions and decisions as well as oversight of information management and destruction of records, with sanctions for non-compliance.
>
> *Investigation Report F-15-03 - Access Denied; Records Retention and Disposal Practices of the Government of British Columbia*, CanLII 2015 BCIPC No. 63

This report makes it clear that other jurisdictions in Canada are dealing with significant issues in terms of both proper record keeping in the first instance (largely as a result of technology such as pin-to-pin messages and texts which allow communications in a form which is not retained or backed up) and in the improper destruction of important government records, in particular email communications. We are naive if we think that similar situations have not happened in this jurisdiction. They just haven't been caught out yet. If the Northwest Territories is doing a comprehensive review of our legislation, it is important to include provisions that addresses these issues, and make these actions a clear offence under the Act with significant penalties attached.

Should the fines associated with the offences be increased? If yes, what amount?

The fine needs to be high enough to act as a true deterrent not only to the individual convicted, but to others. I would recommend fines of between $5,000 and $10,000 if for no other reason than to provide a significant dis-incentive to those who might feel inclined to "cheat".

7.4 Currently the ATIPP Act defines both who the head of a public body is as well as the Minister who is responsible for the administration of the Act. All public bodies are required under the Act to delegate specific processing functions to a position within the public body; however the Act is silent on the position of the Access and Privacy Coordinator.

Newfoundland's legislation has defined the role of the "coordinator" and further detailed functions relating to this position within their legislation

Should the ATIPP Act be revised to identify the position and responsibilities of a public body's Access and Privacy Coordinator?

In the Newfoundland Report, the very first substantive issue addressed is the role of the ATIPP Co-Ordinator. It notes:

> The ATIPP coordinator is at the centre of the process to gain access to information while ensuring personal information is kept confidential. This person coordinates both the processing of the request to a public body and the ensuing response. The coordinator's key role affects the quality of the requester's experience and the consistency with which the ATIPPA is followed.

The recommendations made in the Newfoundland Report in relation to ATIPP Coordinators were twofold:

- that the Act be amended to give delegated authority for handling access to information requests solely to the ATIPP Co-Ordinator

- that no officials other than the ATIPP Coordinator be involved in the request unless they are consulted for advice in connection with the matter or giving assistance in obtaining and locating information

These recommendations were incorporated in the new legislation in Newfoundland.

I have often commented on the fact that in the Northwest Territories the role of ATIPP Coordinator is most often given to someone with a host of additional roles and responsibilities and that the ATIPP work gets done "off the side of the desk" as and when there is time to do it as a secondary job responsibility. I would advocate for a more prominent and professional role for ATIPP Coordinators, including a requirement that they have specialized training in the field. The provisions in the new Newfoundland legislation are a good start to professionalizing this role within government and I would heartily support and **recommend** similar provisions in our legislation.

7.5 ***Although the Access and Privacy Directory provides information regarding the Act and Regulations it does not provide a general listing of records held by public bodies, a practise undertaken by a number of jurisdictions.***

Jurisdictions also require the publication of each public body's personal information banks. Personal information banks include a description of the personal information held by a public body and that it's organized and retrievable either by a person's name or by an identifying number assigned only to that person.

Should the Act include a provision that requires that the Access and Privacy Directory include a general listing of records held by each public body?

Without a good idea about what this entails or how detailed these lists would be, it is difficult to comment on this other than to say it would be impossible to list every record held by every public body. I'm not entirely sure that a list of the types of records held by a public body would be overly helpful. Most individuals who make access to information requests have very specific records in mind when they make their request. They don't really care what form the records take or how the records are classified.

Should the Act be revised to require that public bodies publish personal information banks relating to the personal information in their custody or control?

This is a more interesting idea but, again, it would be difficult if not impossible to maintain a full list of the personal information that public bodies collect, use and

disclose and, in my experience, would not likely be referred to by applicants seeking specific information about a specific matter that concerns them. I have no real feeling, one way or another, as to whether this would improve the general scheme of the ATIPP Act or how it is utilized by the public.

7.6 This section permits public bodies to specify categories of record that are available without an access to information request, however it does not require this to be done. In British Columbia, it is a requirement under their legislation for public bodies to establish categories of information that is available to the public without a formal request.

Should the ATIPP Act be revised to require public bodies to establish categories of information that the public can access without a formal access to information request?

This would be a positive step in the direction of pro-active disclosure and could save time and resources which would otherwise be spend responding to Access to Information requests. I would encourage and **recommend** this amendment.

7.7 Currently there are no provisions within the ATIPP Act that provide a requirement to undertake a comprehensive review of the Act, on a regular basis. The majority of jurisdictions require a review be undertaken, generally every 5- 7 years.

Should the Act be revised to include the requirement for a regular comprehensive review of the legislation? If so, how often should this review happen?

This is the first comprehensive review of the ATIPP Act in 18 years, despite the fact that technology has progressed far beyond anything that was even contemplated in 1997. The volume and the value of information has increased exponentially since 1997. If the legislation is to remain relevant to current trends and technology, I would advocate for and **recommend** a mandatory review of the Act every 5 years.

8. OTHER COMMENTS OR CONSIDERATIONS

8.1 Enforcement of Accepted Recommendations

Once the public body has accepted recommendations made by the IPC, there is nothing in the Act which provides for or allows any follow up or enforcement. I have had a number of Applicants return to me after my role as the IPC is complete (I have made recommendations and they have been accepted by the public body) and ask me to follow up with the public body because they haven't done what they said they were going to do. It's one thing when the issue is an access to information matter and the applicant knows whether or not the recommendations have been followed. It is another matter where the matter involves a breach of privacy. Normally there is no follow up and no obligation on public bodies to report when they have completed the steps

recommended or how they have done so. I **recommend** that an amendment to the Act be made that would require such a follow up on the part of the public bodies.

8.2 Cities, Towns and Villages and other organizations which should be added as "public bodies" under the Act.

As you know, I have been advocating for many years that municipalities either be added as "public bodies" under the Act or that separate legislation be passed to deal with municipalities. Either way, municipalities in the Northwest Territories must become subject to rules and procedures with respect to both access to information and protection of privacy.

I would also strongly **recommend** that other quasi-public organizations be named as public bodies under the Act. Housing Authorities established under the Housing Corporation Act immediately come to mind. They receive much of their funding from government and are required to follow government policy objectives. They also collect and use considerable amounts of personal information. Notwithstanding all this, they do not have any legislated obligations with respect to the collection, use or disclosure of personal information, nor are they accountable to the public through the access to information process. There have been many complaints to my office in the last number of years which arise in one way or another from government funded housing organizations in the Northwest Territories. It is time that they became subject to the access and privacy provisions of the Act.

8.3 Clarification of s. 34(1)

This section provides that "notwithstanding any other Act or any privilege available at law" the IPC may require the production of and examine any record to which the Act applies and that is in the custody or under the control of a public body. While it has not, as of yet, been a significant issue in this jurisdiction (though it has come up) a number of other jurisdictions have run into circumstances in which the IPC has been refused access to certain records because they are claimed to be protected by solicitor/client privilege. In fact, this is an issue which has been litigated relatively frequently in Canada, and which has created a fair bit of controversy. The courts, up to and including the Supreme Court of Canada, have rightly determined that solicitor/client privilege protects the important relationship between a client and his/her lawyer and must be protected. It has also been determined, however, that the privilege is not absolute and will yield in some circumstances. For that privilege to be set aside, there must be very clear and unequivocal wording. That said, for an IPC to evaluate a claim of solicitor/client privilege he/she must be able to see the record. The Newfoundland Report does a very good review of the issue in Chapter 3 (pages 109 to 121). In their analysis of the issue, they make the following observations:

> The Committee shares the concerns of the Commissioner, the Federal Information Commissioner, the Centre for Law and Democracy, and other participants about the apparent ease with which s. 21 can be used abusively. If the Commissioner is unable to examine documents in respect of which the public body claims solicitor-client privilege, he cannot possibly determine the validity of the claim. (Pg 117)

For absolute clarity on this issue, I **recommend** that our section 34(1) be amended to read as follows:

> 34.(1) Notwithstanding any other Act or any privilege available at law, *including solicitor client and litigation privilege*, the Information and Privacy Commissioner may, in conducting a review under this Division, require the production of and examine any record to which this Act applies that is in the custody or under the control of the public body concerned.

8.4 Power to subpeona records

Sections 34(2)(iv) and 49.4 of the Act gives the Information and Privacy Commissioner the power to compel "any person to produce any record to which this Act applies that is in the custody or under the control of the public body concerned". This power, however, ends at the doors of the public body. Particularly in the case of a breach of privacy, in order to be able to prove that privacy has been breached, it may be necessary to collect evidence, including records, from a third party. In at least one review, my office was unable to conclude whether or not there was a breach of privacy because I was not authorized to subpeona the records I required from a third party and the third party chose not to co-operate. I **recommend** that the Act be amended so as to give the IPC the power to subpeona any records relevant to a review, whether that record is in the possession of a public body or a third party.

APPENDIX 1