OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Supplementary Submission of the Information and Privacy Commissioner to the Access to Information and Protection of Privacy Review Committee

August 29, 2014

OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

August 29, 2014

Mr. Clyde Wells
Chair
ATIPPA Review Committee
Suite C
83 Thorburn Road
St. John's, NL
A1C 3M2

Dear Mr. Wells:

During the course of the presentation by this Office to the *ATIPPA* Review Committee, the OIPC was asked by Committee members to further consider or elaborate on certain points which were discussed during the presentation. Furthermore, we have read and listened to the views presented by others during the review process, and we also offer some views here on topics they raised. We have tried to avoid restating positions which are already contained in our primary formal submission to the Committee.

Personal Information in Biological Samples

One of the topics which we were asked to consider by Ms. Stoddart is the issue of privacy protection for biological samples, such as human tissue, DNA, etc. The attached research paper (Appendix 1) is the result of our inquiry and analysis into this issue. We see this as an emerging issue in the privacy world, which will certainly need attention and appropriate legislative development. Our findings lead us to believe that if there is a need for legislative recognition and privacy protection for the personal information contained in biological samples, the most appropriate place to begin that consideration in a small jurisdiction such as this would be during the first statutory review of the *Personal Health Information Act* (*PHIA*), which is mandated to occur in 2016. We believe that very few public bodies subject to the *ATIPPA* are currently engaged in the collection of human biological samples, with the possible exception of law enforcement. Furthermore, given that very few jurisdictions internationally have developed legislation aimed at this area, there are still too many questions as to how best to approach this issue from a legislative standpoint. We commit to revisiting this issue during the *PHIA* review in 2016, and to update our research in this area in order to incorporate new developments.

Timeliness of Responses by Public Bodies to Access Requests

Another issue which came to the fore in our presentation, as well as others, is the issue of timeliness of responses by public bodies to access to information requests. There have been comments from some presenters which may lead to the impression that access to information requests are routinely taking longer than the maximum time allowed under the *ATIPPA*. The ATIPP Office of the Office of Public Engagement has provided some clarification on this issue in its formal submission, which contains statistics showing that compliance with legislative timelines has improved greatly in recent months.

Our Office only deals with files where the applicant wishes to file a complaint or ask us to review a public body decision. Our experience is that since the *ATIPPA* came into force in 2005, from time to time a request for review has come into our Office which was what we refer to as a "deemed refusal" - a request where the public body failed to respond within the legislated time frames, and under section 11(2), the head of the public body is deemed to have refused access to the record. Many of these have been resolved informally over the years through a quick phone call from this Office to the public body. There have been a few more egregious cases in terms of the length of delay, resulting in a report from this Office, such as Report A-2011-010. More recently, in 2012 we noticed an increase in the number of deemed refusal cases coming to our Office for review. This became a serious enough concern that in January of 2013 a news release was issued by this Office in conjunction with a Report on one recent case, which brought the issue into the spotlight.

Subsequent to this news release, we held a meeting with the Minister and senior officials responsible for the *ATIPPA*. Over the next number of months, the issue was essentially resolved. Although we had by that time collected a backlog of over a dozen such cases, by February of 2014 we were able to issue a follow-up news release to indicate that our concerns about response times had been appropriately addressed. No further requests for review or complaints about deemed refusals have come to this Office since then.

It may well be the case that the legislated time lines can be tightened in order to better serve the public. It is quite possible that the first 30 day extension, which can be applied unilaterally by a public body, may be being abused. We see no reason why all such extensions should not have to be approved first by the Commissioner. That being said, we have not encountered a major problem with public bodies not meeting the time frames as they are currently mandated by legislation. If there is such an issue, applicants are not choosing to bring it to our attention.

Centralizing the Access to Information Process within Government

This topic was addressed by Mr. Wells primarily as a means of potentially making the access to information process more efficient. It should be noted that one jurisdiction in Canada, British Columbia, has been operating with a centralized access to information process for about three years. "Information Access Operations (IAO)" is an entity within the Ministry of Technology, Innovation and Citizen Services which is responsible for administering the *Freedom of Information and Protection of Privacy Act* as well as records management and document disposal laws. A complete list of services offered by Information Access Operations is available at
http://www.gov.bc.ca/citz/iao/iao_core_services.pdf

It is our understanding that this initiative was undertaken primarily in response to concerns by the BC OIPC about problems with public bodies meeting response timelines for access to information requests. Our information indicates that while timelines have not improved, there may be a number of factors influencing that number, including a hiring freeze at Information Access Operations. IAO employs approximately 105 people.

Our understanding is that members of the public may send an access request to a public body, or directly to IAO. That entity works with the public body to ensure that records responsive to the request are located and forwarded to IAO, where they are reviewed, with any necessary information being severed, and any records to which the applicant is entitled are forwarded from IAO. IAO is not a decision-making body, however, as final decisions must always be confirmed by the public body having control or custody of the records. Furthermore, we believe it must stand to reason that significant back and forth communication between IAO and the public body may be required, particularly when it involves determining whether a harm threshold has been met, or when considering the exercise of discretion for discretionary exceptions, given that subject matter expertise along with a variety of other considerations would likely be the purview of the originating public body.

Initially when this system was set up, it is our understanding that Access & Privacy Coordinators were moved from the various public bodies to IAO, and they brought with them the requisite expertise in the subject matter often dealt with by those bodies, and furthermore they brought with them an understanding of which individuals and offices within the public bodies would likely have knowledge of the existence or location of records. They also often had an intimate knowledge of the information management systems in use by the public body they had recently departed.

After a period of a few years, however, these assets are no longer present to the same extent in the staff of the IAO. Normal staff turnover and retirements would obviously have some effect over time, but also new filing systems, new staff in the public bodies, reorganizations within public bodies, redistribution of responsibilities among Ministries, etc are all having the result that IAO staff do not have the same intimate knowledge of the function of each public body and understanding of how to assist Ministerial staff in locating and identifying records. The result has been a recent move to re-establish positions within the Ministries to coordinate responses to the IAO regarding access to information matters. Over time, the relationships which may have added value to this process are simply degrading, and any initial efficiencies in the process are difficult to identify when weighed against the time and effort involved in working through what is effectively an additional layer of bureaucracy.

Unless it was set up as some sort of independent office, centralizing the process in this way would not address any of the concerns which have been raised by some presenters that there may be a degree of political interference in the access to information process regarding requests from the media or opposition. On the contrary, a centralized office such as this may evolve into a funnel to the highest levels of government, which in our experience has sometimes been the source of delays experienced by applicants.

It may take several years of additional experience in BC before it can be concluded whether the IAO process has a negative, positive, or neutral effect on timeliness and efficiency for access to information applicants. One distinct advantage is that IAO is composed of a large group of employees with specialized expertise in access to information. Its success or failure may be largely

contingent on appropriate funding to allow for sufficient staffing levels, however that may be the case for either model. We are not convinced that adopting a model such as that which is found in BC is the most pressing need, nor will it necessarily solve more problems than it might create.

Our recommendation regarding the administration of *ATIPPA* within the line departments of government is to professionalize the position of ATIPP Coordinator to the extent possible. We find that our experience with ATIPP Coordinators varies from department to department within government. Some seem to function at a low level within the departmental hierarchy. They appear to be delegated very little responsibility and are essentially carrying messages back and forth from someone higher in the organization, and often cannot explain the rationale for positions adopted by the department. On the other hand, we also deal with departmental access coordinators who are knowledgeable and experienced, and who are clearly fully engaged with senior decision makers within the department and can therefore speak to all aspects of a matter when it comes under review by our Office. There must be a way to ensure that ATIPP Coordinators are given a greater role in the process, and allowed to bring their knowledge and experience to bear in a leadership role in the ATIPP process. There are nationally and internationally recognized professional certifications available to those who work in that area, and this is something which could be further investigated. We believe this can be accomplished without revamping the entire ATIPP structure within government.

Another recommendation we would like to make is that the ATIPP Office should be empowered to advise and provide training to not only core government departments and agencies, but also to municipalities. We question whether the Department of Municipal Affairs is the most appropriate agency to provide *ATIPPA* compliance advice to municipalities, particularly when specialized expertise already exists within the ATIPP Office of the Office of Public Engagement. We plan to engage with the Office of Public Engagement and stakeholders in the municipal sector in the early fall to discuss how best to move forward and create a better understanding of the role and purpose of *ATIPPA* within the municipal sector.

Posting of Completed Access Requests on the Office of Public Engagement Website

As part of the Open Government initiative, it has been the recent practice of government to post completed access to information requests online following a 72 hour waiting period after information has been sent to an applicant electronically, and 5 days after it has been sent by mail. We have heard informally from journalists since that practice was begun that it can be a deterrent to investigative journalism when a journalist is the applicant.

From our understanding, the access to information request can be part of a larger investigative process, and the response to the access request may be followed by further research or interviews, and finally the process of writing the article and having it published or broadcast. The incentive to pursue these projects can be undermined when other news outlets or bloggers can access the records, into which the applicant's news organization may have invested time, money and energy, within 72 hours of the journalist receiving it. The result is that the journalist may not be the one to "break" the story, and editors and publishers will not be as interested in pursuing similar projects in the future. While the practice of publishing completed access to information requests is a good one that we fully support, we are of the view that lengthening the period of time before publication would actually encourage and support the purpose of the legislation, which, under section 3, is to

make public bodies more accountable. We therefore propose that the current waiting period be doubled before publication by government of completed access to information requests.

Fees

There are two types of fees involved in the access to information process. There is a $5 application fee, and there are also fees which may be charged for providing records to an applicant. In our formal written submission to the Committee, we discussed the issue of fees with a view to ensuring that our fee regime was the most affordable and least onerous in Canada. During our initial presentation and in some of the presentations that followed, there was some discussion about fees, and as a result we have conducted some additional research on the subject (Appendix 2).

We now recommend the elimination of all fees for access to information. It is clear that the time and effort involved in estimating, assessing, and processing fees by public bodies is more of a burden than a boon to them, while the time involved in administering the fee regime as well as the fees themselves are a deterrent to Applicants. Any concerns that the elimination of fees may result in public bodies becoming overburdened through limitless access to information requests can be addressed through the application of section 43.1 to disregard such requests.

Order Power for the Commissioner

Currently under the *ATIPPA* the Commissioner has the power to make recommendations, but no power to issue an order. The OIPC does, however, have the ability to appeal a decision of a public body to the Supreme Court, Trial Division if the public body chooses not to follow our recommendation. Our current model of oversight is known as the "ombuds" model.

In our formal written submission to the Committee, we did not recommend an amendment to the *ATIPPA* in order to provide the Commissioner with order-making power. We have found the ombuds model to be a workable one, and our assessment of the *ATIPPA*, particularly following the Bill 29 amendments, was that there were a number of higher priority amendments which we believed must take priority, ahead of any consideration of order power for the Commissioner. Indeed, a large proportion of our written submission focused on ways to increase the effectiveness of *ATIPPA* oversight.

During our initial presentation, the Committee challenged us to consider whether the ombuds model was the most effective approach to oversight. We also observed, during the course of the Committee's hearings, that a number of presenters indicated that there was to some extent a lack of confidence in the oversight function based on the perception that the Commissioner is "toothless". Although we have a strong record of taking cases to court when we believe there is a public interest in doing so, we acknowledge that from an applicant's point of view it is not an efficient process. Furthermore, we also acknowledge the assertion by Federal Information Commissioner Suzanne Legault that public bodies would have a much greater incentive to participate more fully in the review process, both at the informal resolution level and the formal submissions stage, if the Commissioner had the power to issue a binding order. Over the years we have noted a great degree of variability in the level of commitment by public bodies to both the informal and formal review process, which undermines the credibility of the process. If order-making power can provide the necessary incentive for public bodies to engage with us during the review process as fully as they would with a judicial process, then we can see significant benefits for better oversight of the law.

This model should also restore confidence that the Commissioner's review process is productive and worthwhile for applicants.

As we indicated in both of our presentations to the Committee, however, we believe that there are a number of arguably more pressing issues relating to the Commissioner's oversight of the *ATIPPA* which must be addressed. Specifically, we have argued that the *ATIPPA* must be amended to make it absolutely clear that the Commissioner can conduct a review of any denial of access to information by a public body, and be able to access any records relevant to such a review, including information or records withheld pursuant to claims of sections 5, 18 and 21. Furthermore, we have argued that the Commissioner's current powers with respect to privacy oversight are very limited and ineffective, and our recommendations to boost those powers are clear. To give the Commissioner order-making power without also implementing our recommendations in respect of these other two areas would only amount to a marginal improvement in the oversight function. It may even be counterproductive, as it might leave the impression that oversight has been significantly improved when it has not.

A final note with regard to this topic is that we ask the Committee to be mindful in its recommendations that this is a small office which has oversight of both *ATIPPA* and *PHIA*. Any model of oversight which would require a high degree of stratification and specialization within the Office could negatively impact our ability to be flexible and apply resources where the need is greatest, whether that be *PHIA* or *ATIPPA*, depending on the caseload and issues of the day. This is an area where, should the Committee make a recommendation in favour of order-making power, perhaps it could also be accompanied by a recommendation that consultations be undertaken by government with the OIPC before the draft legislation is tabled.

As a result of our participation in the hearing process, as well as listening to the concerns of other presenters, it is fair to say that our thinking has evolved on this issue, and we are now in favour of an amendment which would result in order-making power for the Commissioner, provided that such an amendment is made under the right conditions, as outlined above.

Public Interest Override

In our supplementary presentation to the Committee on August 21st, we were asked to provide further information on the subject of our recommended amendment to section 31, the Public Interest Override provision. In our formal written submission we recommended what we believe to be a strengthened version of this provision, modelled on the one found in British Columbia. The purpose of such a provision is to create a positive obligation on public bodies to disclose information that is clearly in the public interest to disclose despite any provision of the *ATIPPA*.

The BC Information and Privacy Commissioner, Elizabeth Denham, has issued several reports regarding public interest override that highlight key considerations for Newfoundland and Labrador. Investigation Report F13-05, *Public Body Disclosure of Information Under Section 25 of the Freedom of Information and Protection of Privacy Act*, was released in December 2013. This review was prompted by a request from the BC Freedom of Information and Privacy Association, based on a submission by the University of Victoria's Environmental Law Clinic. The Commissioner reviewed five case studies involving public bodies that may have failed to disclose information pursuant to Section 25 (Public Interest Override) of BC's *FIPPA*. In addition, the Commissioner surveyed 11 public bodies regarding any policies and procedures they have in place to comply with Section 25.

Of the five case studies, the Commissioner identified one where the ministry failed to meet its obligations under Section 25. It is interesting to note that the risk involved in that case was initially noted years before the *FIPPA* was proclaimed; the Commissioner found that the public body should have disclosed the risk once the *Act* was passed. However, in examining the remaining case studies, the Commissioner recommended that the wording of Section 25(1)(b) be amended to remove the "urgent circumstances" that are currently required for public interest disclosure. She recommends amendments that mirror Ontario's *FIPPA*; the Commissioner comments: "application of the public interest override in the Ontario *Act* requires that there be a public interest in disclosure, that the public interest be compelling, and that the compelling public interest clearly outweighs the purpose of the exemption."

As for the survey of public bodies, the Commissioner found that overall, public bodies do not understand their obligations under Section 25. Recommendations included developing policies that provide guidance on Section 25, as well as education on both the policies and Section 25 itself.

The leading case for Section 25 in British Columbia is Order 02-38 issued in 2002 by then-Commissioner David Loukidelis. In that order, the Commissioner made findings in relation to the application of the burden of proof to the public interest override provision. In addition, he interpreted Section 25(1)(b) to be triggered when there is an "urgent and compelling need for public disclosure" and that the Section 25(1) requirement for disclosure "without delay" introduces "an element of temporal urgency." When interpreting Section 25 in its entirety, he concluded that it applied when circumstances are "...of a clear gravity and present significance which compels the need for disclosure without delay."

We conclude that the most recent consideration of the subject by Commissioner Denham, noted above, has value for this jurisdiction, and we concur with her recommendations.

Solicitor-Client Privilege

We would like to briefly comment on the submission of the Office of Public Engagement in relation to the subject of the Commissioner's authority to review claims of solicitor-client privilege. In its submission, the OPE offered an interpretation of the decision by the Court of Appeal in *Newfoundland and Labrador (Information and Privacy Commissioner) v. Newfoundland and Labrador (Attorney General)*, 2011 NLCA 69. The OPE submission states that the Court of Appeal determined that "the language [in the *ATIPPA* prior to Bill 29] was ambiguous and broad enough to include solicitor-client privilege." In fact, the Court's conclusion was quite the opposite. The Court of Appeal determined that there was a key distinction between the language of *PIPEDA* and that of the *ATIPPA* as it was prior to Bill 29, and that the language in the *ATIPPA* in respect of the Commissioner's authority regarding the review of claims of solicitor-client privilege was, in contrast to *PIPEDA*, both explicit and "not ambiguous":

> *[75] Subsection 52(3) of ATIPPA, in contrast to PIPEDA, does advert to issues raised by privilege. While it does not employ the words "solicitor-client privilege", I am satisfied that the words actually employed are not ambiguous and are sufficiently explicit to include that privilege.*

Further to the analysis of the *Blood Tribe* decision offered by the OPE in relation to this issue, it is important to reflect on two important considerations. One is that the *Blood Tribe* decision is in respect of a different piece of legislation with a different purpose, and the second is that the Court of Appeal was cognizant of this fact, having engaged in some analysis of those differences, including the following commentary:

> *[73]It is useful at this point to distinguish ATIPPA from the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 ("PIPEDA"), which was considered in Blood Tribe. Unlike the federal Access to Information Act which, as in the case of ATIPPA, deals with documents in the possession of the government, PIPEDA deals with information in the hands of the private sector.*

The distinction made by the Court of Appeal between *PIPEDA* and *ATIPPA* is crucial to any analysis of this issue. The core purpose of the *ATIPPA*, as found in section 3, is one of accountability of public bodies, rather than protection of consumer rights as in *PIPEDA*. Furthermore, the Court found that the language in *ATIPPA* prior to Bill 29 was "sufficiently explicit" to allow the Commissioner to review claims of solicitor-client privilege. If government was of the belief that the Court of Appeal decision was flawed, it could have sought leave to appeal to the Supreme Court of Canada. Instead, the choice was made to accomplish its purpose by amending the *Act*. We share the view of the Court of Appeal that in order to accomplish its purpose, the *ATIPPA* must allow for a review by the Commissioner of any denial of access to information by a public body, no matter what the reason, including a claim of solicitor-client privilege.

Staff Qualifications and Office Security

In his presentation to the Committee, Deputy Minister Paul Noble of the Department of Justice questioned both the professional qualifications of our staff and the level of security in place at the Office of the Information and Privacy Commissioner. I wish to reiterate for the record that all seven Analysts who are permanent employees of the OIPC hold law degrees. Combined, our Analysts have several decades of experience in a wide range of legal practice areas, and we are pleased to be able to bring their high level of expertise to bear in all aspects of *ATIPPA* and *PHIA* oversight.
Mr. Noble also speculated that solicitor-client privilege might be at risk if we were to consult an outside lawyer in the course of reviewing a claim of that privilege by a public body. First of all, we have never consulted an outside lawyer in relation to any file during our review process. We believe we have the necessary experience and expertise available in our Office to perform this function ourselves, including reviewing claims of solicitor-client privilege, as we did on over 50 occasions prior to the initial court challenge by government of our authority to do so. We do not anticipate ever requiring the services of outside legal counsel in performing our core function, however even in the very unlikely event that we were to do so, I believe we would be able to bring to bear a sufficient level of professional responsibility to take appropriate precautions to ensure the protection of any privilege claimed over the records.

In relation to questions raised by Mr. Noble and others about our level of security, we are of the view that we have an appropriately high level of technical, physical and administrative security in place which provides full protection to all of the information held by our Office. As part of our mandate, we have in fact reviewed and provided recommendations regarding the security arrangements of public bodies under *ATIPPA* and custodians under *PHIA*, and we believe we have some degree of expertise in that regard. We stand on our record in this respect, however we invite Mr. Noble to direct any questions he may have about our security arrangements to our Office.

Information Security

In its written submission, the OPE proposed that section 22(1)(l) be strengthened in order to better protect against disclosure of information about security arrangements. In particular, the submission listed the jurisdictions of Nova Scotia, Ontario, Manitoba, Alberta, British Columbia, and Nunavut as having access to information laws with stronger protection against disclosure of this type of information.

Our reading of this recommendation is that any such amendment would actually result in more information being released in relation to security arrangements than is currently the case with the present version of the provision. All of the other jurisdictions cited by the OPE include a harms-based element in the exception to access, such that a public body may only refuse to disclose information about information security if the disclosure would cause harm to security. As a result, the public body would be obligated to disclose any information about security which would not meet the threshold of harm, which is usually interpreted to be a "reasonable expectation of probable harm." Any public body responding to an access request which was not able to discharge the burden of proof in that regard would have to release the information requested.

In this jurisdiction, however, we already have a very strong exception in 22(1)(l), because it allows the public body to withhold all information that "could reasonably be expected to reveal the arrangements for ... security." It is not necessary, under this provision, for a public body to assert that disclosing the requested information would cause harm. Rather, they must simply prove that the requested information, if disclosed, would "reveal" information about security. Even if disclosure of the information would not cause harm, the public body is still entitled to withhold it. This is a much lower threshold to meet if the intention is to withhold information about security. In the interests of greater security for the personal information and third party business information holdings of public bodies, we recommend that the current provision be maintained.

Policy or Practice of MHA Inquiries Being Routed Through the Executive Assistant to the Minister

In May of 2013 we received a complaint from an opposition MHA, Ms. Gerry Rogers. Her concern was that a policy or practice had been put in place by government (and in particular by Minister Joan Shea) which disallowed Members of the House or their staff from contacting employees of departments and agencies in the course of assisting a constituent. She had several concerns with this policy or practice, but there was a privacy aspect which we agreed to consider and comment on. We could not accept this as a privacy complaint under section 44, however, because the language of that provision is limited to individuals complaining about misuse of their own information. Ms. Rogers was instead complaining about the use or disclosure of the personal information of her constituents to a Minister's Executive Assistant, when in fact the constituent had not given any consent for employees in the Minister's office to become involved in their personal affairs. In making inquiries into the matter and in writing a letter to Minister Shea which was copied to Ms. Rogers (Appendix 3), we relied on the Commissioner's authority in Section 51(a) to "make recommendations to ensure compliance" with the *ATIPPA*. Although we were not obstructed in making our inquiries, it is noteworthy that we were unable to engage the Minister in any consideration of our findings. Although we requested a reply, none was forthcoming.

As you can see from our letter, we supported the government policy of requesting that Members seek written consent from constituents when practicable in order to inquire into the constituent's personal matters. Although not required by statute, we were of the view that such a policy helps to ensure that the correct constituent is identified, and that the public body will only disclose the information necessary regarding the constituent to allow the MHA to assist the constituent in the particular matter requested. We were also clear that the lack of such written consent should not be used to interfere with the MHA's work in urgent cases.

We were also unable to say categorically that there should never be a case when MHAs are asked to deal with the Minister's Office directly regarding a constituent inquiry in complex cases involving unsettled policy matters or Ministerial discretion. We were given to understand by Ms. Rogers, however, that the majority of the constituency work undertaken is of a more routine nature. On that basis, we were of the view that the policy or practice reported by Ms. Rogers was not in compliance with the *ATIPPA*. We indicated as much in the letter written by a staff person from this Office, and owing to the Commissioner's limited ability to compel compliance, or even a response, in relation to privacy matters, the matter ended with our letter to the Minister.

Directory of Information

Section 69 mandates the creation of a directory of information to assist in identifying and locating records in the control or custody of public bodies. In the interests of making the *ATIPPA* more "user friendly", we believe that such a directory could be enormously helpful to applicants, and indeed it could result in fewer formal access to information requests, on the basis that the information would be readily located and accessible. We believe that this provision is very much in line with the Open Government Initiative, as well as the purpose of the *ATIPPA* as outlined in section 3(1)(a) of giving the public a right of access to records.

We acknowledge the concerns expressed by the OPE that it may not be practical to require outside agencies such as health and educational bodies and municipalities to develop such directories, however we believe it is achievable for the line departments of government to do so. In fact, section 69(5) indicates that this section only applies to those public bodies listed in the regulations. The line departments of government could be added one at a time over an appropriate period of time as the template for such a directory is developed and applied to each. Such a directory could be maintained online, and once established would simply need to be updated as required.

Notification to Individuals when Personal Information is to be Released in Response to a Request

It has been noted by this Office and other presenters to the Committee that the current version of section 30 (personal information) is much improved from the version which existed prior to the Bill 29 amendments. During our presentation on August 21st, it was noted by Ms. Stoddart that there exists in British Columbia and elsewhere a provision for notification of individuals (third parties) in cases where the public body intends to disclose information to an applicant which might contain personal information.

Such a notice provision comes into play in the equivalent to section 30 when the public body, having considered all of the factors to be weighed, is of the view that even though the balance tips in favour of disclosure, there remains some reason to believe that such a disclosure might not be in

compliance with the law. Upon reaching such a conclusion, the public body must notify the third party of the intended disclosure and invite representations from that individual. The framework in both BC and Ontario for implementing this notice is essentially the same as for notifying third parties where a third party business interest may be affected, which occurs under section 28 in *ATIPPA*. As with third party businesses, the personal information notification provision includes standing to appeal to the Commissioner and then on to Court.

The legislation in Ontario and British Columbia provides for notification to individuals when their personal information is to be released when there is a question about the applicability of the exception. In BC the section specifically states in section 23(1):

> *If the head of a public body intends to give access to a record that the head has reason to believe contains information that might be excepted from disclosure under section 21 or 22, the head must give the third party a written notice…*

In Ontario, the test in section 28(1) is as follows:

> *Before a head grants a request for access to a record,*
> *(a) …*
> *(b) that is personal information that the head has reason to believe might constitute an unjustified invasion of personal privacy for the purposes of clause 21 (1)(f),*
> *the head shall give written notice in accordance with subsection (2) to the person to whom the information relates.*

Both jurisdictions also provide for notice on a permissive basis where the information is not going to be disclosed.

The BC OIPC has found that "a mere possibility [of an unreasonable invasion of personal privacy] triggers the obligation to consult" in Order No. 233-1998. However, that is tempered by the finding that "there must be a reasonable basis for that belief".

The Ontario OIPC found in Investigation Report I98-018P that notification must occur every time the public body intends to rely on a sub-section addressing "not an unreasonable invasion" (our section 30(2)) and "there is a reasonable doubt as to whether the requirements of these exceptions have been established". This would appear likely to result in a larger number of notifications under the Ontario provision.

The experience of the BC OIPC with their section is that in most cases public bodies err on the side of caution when it comes to claims of personal information, and as a result very few notifications of release are sent to individuals, and even less frequently are appeals filed with the OIPC. Therefore the addition of a similar provision would likely not result in an unreasonable burden on public bodies or on this Office.

However, one must examine the relative value of adding such a provision. The balancing exercise now present in section 30 is relatively new, being first introduced only two years ago. Our view is that we now have, for the first time, a workable personal information exception, owing to the Bill 29 amendment. Based on the relatively low usage in British Columbia, it is not clear that adopting that model would result in significant benefits. At the same time, adopting the Ontario model might

result in greater challenges with implementation for public bodies. It is therefore questionable whether this further amendment to section 30, at this particular time, would yield positive results, particularly when we already have a much improved, workable provision. It should also be noted that this provision only applies when the possible disclosure of personal information is triggered by an access to information request. Other disclosures of personal information for specific purposes are provided for in Section 39 of the *ATIPPA* which does not require notification.

We neither recommend nor oppose such an amendment to the *ATIPPA* in theory, however in practice we do not believe that it warrants consideration in this review process among some of the more important amendments being proposed. Certainly, while we were aware that the *ATIPPA* lacks such a notification provision as we prepared our formal written submission to the Committee, it was not considered a pressing enough issue to include for consideration. We remain of that view.

Mandatory Reporting of Privacy Breaches to the Commissioner

During our presentation to the Committee on August 21st, Mr. Letto asked us to consider the effect of an amendment to the *ATIPPA* which would require public bodies to report all privacy breaches to the Commissioner. In our formal written submission to the Committee, we requested that the *ATIPPA* be amended to provide for a requirement for breach reporting to the Commissioner, however we were not specific as to the threshold for such a reporting requirement, ie, whether it would be a requirement to report all privacy breaches, or just those which are considered to have met the "material breach" threshold, as found in *PHIA*. We did note, however that there might be different considerations under *ATIPPA* as compared to *PHIA*.

Under *PHIA*, we have oversight of all custodians of personal health information. While the Regional Health Authorities are the largest custodians by far, there are thousands of small custodians, composed largely of regulated health professionals in private practice. The material breach threshold in *PHIA*, or something like it, is probably appropriate for oversight of such a large number of custodians. There are difficulties inherent in providing oversight of such a large number of disparate bodies, and even if custodians under *PHIA* were required to report all breaches, it might be a challenge to continue to make sure they were aware of this obligation.

Oversight of public bodies is different, however. Government departments and agencies, crown corporations and municipalities are accustomed to regulation and oversight in a way that private corporations are not. There are strong institutional connections and bureaucratic practices which facilitate, generally speaking, a greater awareness of and relationship to various forms of legislated oversight. On that basis, we have given the matter further consideration and we are of the view that it would be an achievable goal to require that all privacy breaches experienced by public bodies be reported to the Commissioner. The current policy of the OPE is that breaches should be reported to the ATIPP Office, so we see no additional burden for public bodies to make the same report to the Commissioner.

In its written submission the OPE indicated that in the first six months of 2014, 39 privacy breaches were reported to the ATIPP Office. Of these, 30 were deemed to be minor in nature, while 9 involved more sensitive information. Having knowledge of the types of breaches and the actions being taken by public bodies to respond to these breaches would be helpful to our Office in discharging our oversight function, because it would allow us to identify trends and problems and to address such issues from an oversight perspective. In that sense, we likely would not take any action

or require anything substantive of public bodies in relation to the minor breaches, particularly as they would also be engaging advice from the ATIPP Office. The value in learning of them would be largely in our assessment of the "big picture." In terms of being notified of the more serious breaches, we would still expect and encourage public bodies to work with the ATIPP Office and to use the steps in their privacy breach protocol, however we would also be able to monitor the situation, and in certain circumstances initiate an investigation where warranted. We could also engage in a discussion with the public body around any decision to notify affected individuals. We reiterate our support for privacy breach notification to affected individuals, and privacy breach reporting to the Commissioner. We do not anticipate any difficulties with accepting and working with a mandatory privacy breach reporting provision which would require public bodies to report all breaches to the Commissioner.

Third Party Business Interests (Section 27)

One suggestion which was discussed in some of the presentations was the notion of adopting the United Kingdom model of the Third Party Business Interests provision. We have examined the UK provision, and while we appreciate the apparent simplicity it presents, it should be borne in mind that the detailed guidance available in the UK on the interpretation of that provision is the result of it being in force in that country for a long period of time, and no doubt subject to many years of legal challenges and rulings.

Similarly, the three part test in Canada is a long-standing, widely used provision in access to information law, and it has been interpreted by the Supreme Court of Canada as well as lower courts and Commissioners across Canada for many years. As Information Commissioner Suzanne Legault pointed out, the experience in the federal jurisdiction with the three-part test is that in the early years it resulted in a large number of court cases initiated by businesses, however as time has gone on and the interpretation of many aspects has settled, it has now become a well understood and accepted provision in the business community.

Interestingly, we note that through the course of the *ATIPPA* Review process, presenters representing the business community have come out in favour of a return to the three-part test, because it is well understood and it allows for transparency and greater competition for contracts in the public sector. The reluctance we have seen to return to that model has largely been from government departments and agencies, which is noteworthy given that the purpose of the provision is to protect the interests of private businesses.

The risk of going to a unique version of section 27 which has not been found anywhere else in Canada is that we could see a repeat of the experience noted by Ms. Legault, where businesses find they must take everything to court because they want to know how a Canadian court will interpret the provision. Even though there would no doubt be significant jurisprudence from the UK context, it is possible that courts in this country will find that they need to consider the specific language along with the overall purpose and context of Canadian legislation as well as the jurisprudence on access to information in general in this country, which may or may not diverge from the UK in key areas. As a result, it may be that an apparently simpler provision on the surface may lead to a much more troublesome provision, and the burden of using this provision will be borne by the business community as it initiates appeals and reviews in order to establish precedents for a new provision in Canadian access law.

Finally, it must be remembered that the three part test to which we advocate a return is in place at the federal level in this country, as well as in Nova Scotia, PEI, Ontario, Alberta and British Columbia, and it has been in place in those jurisdictions in some cases for 30 or more years. It has been tried and tested, and it strikes the right balance in order to protect the legitimate interests of the business community in this province.

Section 8.1 of the Evidence Act

We have reviewed written submissions provided to the Committee from the Canadian Medical Protective Association (CMPA) and the Healthcare Insurance Reciprocal of Canada (HIROC) which address concerns about the operation of section 8.1 of the *Evidence Act* in the *ATIPPA* Regulations. As noted in our previous written submission, there are a number of provisions listed in section 5 of the *ATIPPA* Regulations for the purpose of designating that the listed provision prevails over the *ATIPPA*. Section 8.1 of the *Evidence Act* is listed there, however it is another example such as those referenced in our formal submission of a provision which does not accomplish what was perhaps intended. The *Evidence Act* ensures in section 8.1(3) that peer review and quality assurance records "shall not be disclosed in or in connection with a legal proceeding." The term "legal proceeding" is a defined term in section 8.1(1), and it does not include an access to information request. Therefore, it has been the view of this Office for some years that the inclusion of section 8.1 of the *Evidence Act* in the *ATIPPA* regulations serves little purpose.

This state of affairs prompted the decision to include within *PHIA* a provision which would more clearly exempt from disclosure information relating to peer reviews and quality assurance reviews. Even that law, however, is limited to some extent as to what can be protected from disclosure. Section 58(1)(c) of *PHIA* requires a custodian to refuse to grant access to an individual who wishes to examine or receive a copy "of his or her own personal health information" which may be contained in such a record.

As a result of section 58(1)(c) of *PHIA*, an individual would not be able to access their own personal health information in such a record. Section 58(1)(b) ensures that an applicant under *PHIA* cannot receive another person's personal health information. The issue is, however, that there may be information in such records of a general nature regarding policies and procedures, including commentary from medical professionals who have participated in these reviews about the extent to which they have followed such procedures, as well as commentary about their professional practices in general. Unless such information was associated with a particular occurrence or patient, it is not entirely clear that *PHIA* would provide full protection against disclosure of such information, because any information in the control or custody of a regional health authority, which is also a public body under *ATIPPA*, would be subject to a request under the *ATIPPA*. The *ATIPPA*, as noted, lacks protection from disclosure for such records because the matter has not been adequately addressed through the simple inclusion of section 8.1 of the *Evidence Act* in the *ATIPPA* Regulations. It should be noted that even though this is the case, it is possible that other exceptions under *ATIPPA* may apply. For example, some information in such a record might contain the work history or other personal information of medical professionals which could be protected by section 30, or it may contain advice or recommendations protected by section 20.

Although we acknowledge the concerns presented by CMPA and HIROC, we question the solution proposed by CMPA. CMPA expresses the view that section 58 of *PHIA* provides broad protection against disclosure of such records, while our view is that the access provisions of *PHIA* only apply

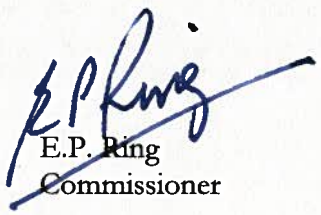
to individuals who are requesting access to their own personal health information, and therefore the exception in section 58 of *PHIA* can only restrict that particular right. Nothing in *PHIA* can restrict access to information which is not personal health information as defined in section 5 of that *Act*. If the Committee wishes to address this issue, we submit that the solution proposed by CMPA of simply listing section 58 of *PHIA* in the *ATIPPA* regulations would serve no purpose, as it would not result in any protection for records which are not the personal health information of the applicant, and such information is already protected from disclosure in *PHIA*. Furthermore, not all public bodies under *ATIPPA* are custodians under *PHIA*.

As noted by HIROC, "it is conceivable that there may be a quality or peer review that would fall under the domain of *ATIPPA* as opposed to the *PHIA*." Their view is that the *ATIPPA* should be amended "in line with section 58 of *PHIA*." We are of the view that nothing can be done by way of regulation to address this issue, if the Committee believes it should be addressed, because there is no existing provision in another piece of legislation which could be added to the *ATIPPA* for the purpose of prevailing over the *ATIPPA* in order to fully protect from disclosure all of the information described in section 8(2)(b) and (c). The only solution, should the Committee wish to recommend one, would be an amendment to the *ATIPPA* which would protect from disclosure to an applicant any information of a quality assurance or peer review as described in the *Evidence Act*.

Conclusion

We wish to thank very much the Committee – Mr. Wells, Ms. Stoddart and Mr. Letto – for listening to us and debating with us the many points, concerns and recommendations we have brought to bear. The *ATIPPA* is certainly being properly and thoroughly reviewed in a balanced, impartial and fair manner, and that is all we can ask. The fact that such a well-qualified and independent Committee was appointed and given such a broad mandate is also a tribute to the leadership of Premier Marshall, without whom the *ATIPPA* may have been destined to continue on under the cloud of Bill 29. I also wish again to acknowledge the excellent work of my staff in assisting with the preparation of this supplementary submission, as well as our initial formal submission to the Committee, and I also extend thanks to the supporting staff of the Review Committee, who have been generous with their time and assistance. Should there be any further questions or clarifications required as the Committee proceeds with its work, please contact me at your convenience.

Yours truly,



E.P. Ring
Commissioner

Enclosures

APPENDIX 1

ATIPPA Review 2014

Access to Information Fees

Introduction

Newfoundland and Labrador currently charges a $5 application fee for access requests; the fee must be paid before the requests will be considered. Most jurisdictions in Canada, with the exception of Quebec and New Brunswick, charge up-front fees to accompany any access request. According to the Office of Public Engagement's *Access to Information and Protection of Privacy Act Annual Report* 2012-13, 660 requests for general access and personal information were received in 2012-13, an increase of 23% from previous years. These requests resulted in $2860 in application fees.[1]

The *Council of Europe Convention on Access to Official Documents* asserts that charging up-front fees for information requests violates international standards; individuals should not be charged to exercise a fundamental right.[2] The Centre for Law and Democracy recommends that up-front fees accompanying requests should be eliminated; globally, 16 out of 95 countries charge up-front fees.[3]

While Section 11(1)(a) of the federal *Access to Information Act* allows up to $25 in application fees, regulations have established the fee at $5. Canada's Information Commissioner has recommended that requesters should not have to pay any fees when a government institution fails to meet a deadline and suggests fee waivers in a variety of situations, such as the public's interest in the information to be released.[4]

A 2011 article in the Globe and Mail indicated that the up-front fee can have a dramatic impact on the number of access requests.[5] The article noted that, when Nova Scotia increased its application fee for access requests from $5 to $25, the number of requests dropped by about a quarter in the following years.

If an increase in fees reduces the number of requests submitted, there may be a concern that removing all application fees would increase the number of applications. New Brunswick announced that all fee would be abolished as of August 5, 2011.[6] The *Right to Information Annual Report* produced by the New Brunswick Department of Government Services reports an increase in access requests as follows:[7]

Year	Number of Access Requests
2012-13	462
2011-12	431
2010-11	370

Processing Fees

Under the *Access to Information and Privacy Act (ATIPPA)*, the current fee structure is:[8]

- an application fee of $5, payable by cheque; individuals requesting access to their own personal information need only pay the application fee;
- $25 for each hour of person time after the first four hours, for locating; retrieving; providing; manually producing; and severing, which includes the review of records to determine whether or not any of the exceptions to access apply, and the subsequent redaction of the records if necessary;
- 25 cents a page for a copy of the record when it can be done using conventional equipment, actual cost when not; and
- actual cost is charged for producing a record in its electronic format and for shipping.

The provincial policy and procedures manual for *ATIPPA* notes that copying fees should not be charged for pages that are withheld in their entirety (i.e. fully severed). However, time spent reviewing, contemplating and severing may still be charged for these pages.

In 2012-13, the Government of Newfoundland and Labrador (Departments and Public Bodies) collected a total of $4663.95 in processing fees.[9] While there have not been many Commissioner Reports stemming from fee complaints in this province, this can be misleading. The Commissioner is unable to issue a report based solely on a fee complaint because such complaints are covered by Section 44(b) of *ATIPPA*. However, fee complaints may be mentioned in reports addressing other complaints under the *Act*.

In British Columbia, the fee schedule differentiates between individual and commercial applicants.[10] The United States *Freedom of Information Act* also bases fees on various categories of requesters, including those intended for commercial use, as well as from educational institutions, noncommercial scientific institutions, news media, and all other requests.[11] The US does not charge an application fee, but once an applicant approves an estimate for the overall request, the fee must be paid even if no responsive records are located or if all the record is severed.[12] Quebec also has a complicated fee regime when releasing documents.[13] For example, municipal bodies charge based on the type of record being requested, differentiating between nine different types of documents. These fee regimes may unnecessarily complicate the request process.

As previously mentioned, in 2011 the Government of New Brunswick removed all fees for access to information requests. This was the result of an election promise, which was also mentioned in the Speech from the Throne. Reference to fees has remained in Section 80 of the *Right to Information and Protection of Privacy Act (RTIPPA)*, with the regulations containing fee structures repealed.

While the number of access requests has not increased dramatically, anecdotal evidence indicates that the breadth of requests is starting to become problematic. Section 15 of *RTIPPA* states

> *On the request of a public body, the Commissioner may authorize the head to disregard one or more requests for access if the request for access*

(a) would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the request or previous requests,

(b) is incomprehensible, frivolous or vexatious, or

(c) is for information already provided to the applicant.

Section 43.1 of *ATIPPA*, by contrast, provides more ability for the public body to disregard requests based on a narrow set of circumstances that assist in preventing abuse of the process:

43.1 (1) The head of a public body may disregard one or more requests under subsection 8(1) or 35(1) where

(a) because of their repetitive or systematic nature, the requests would unreasonably interfere with the operations of the public body or amount to the abuse of the right to make those requests;

(b) one or more of the requests is frivolous or vexatious; or

(c) one or more of the requests is made in bad faith or is trivial.

(2) Where the head of a public body so requests, the commissioner may authorize the head of a public body to disregard a request where, notwithstanding paragraph (1)(a), that the request is not systematic or repetitive if, in the opinion of the commissioner, the request is excessively broad.

The removal of fees in New Brunswick gave rise to another issue – how to differentiate between formal and informal requests. In response, regulations were passed containing information required for a request to be considered an official request.

The *Council of Europe Convention on Access to Official Documents* does provide for fees to be charged for copies of official documents. Section 7(2) notes that "A fee may be charged to the applicant for a copy of the official document, which should be reasonable and not exceed the actual costs of reproduction and delivery of the document." In other words, only photocopying and postage charges are permitted. Advocates also support making records available in electronic formats, reducing the actual cost of copying and delivery.

This is in line with international standards. The UN Human Rights Committee has indicated that in no circumstances may fees be charged which would "constitute an unreasonable impediment to access to information."[14] Further, the organization is of the view that access fees should reflect the cost incurred by the public body in copying and delivering the requested material.[15]

In a 2006 global survey, Privacy International indicated that "the best practice is to limit fees to actual costs for providing information, not for the time taken in deciding on whether exemptions should apply, provide waivers for information of public interest, and not charge for appeals. A general principle adopted in all jurisdictions is that fees should not be used as a barrier or a profit-making device." [16]

Much of the available literature argues that, if providing access to information is part of the government's core role, then fees should not be charged. Proponents for reducing and/or removing access fees argue that the fees create a barrier to access, are undemocratic if access is a right, and reflect a practice of double billing, as citizens have paid taxes that go towards developing the records. Access fees also highlight inequalities; requesters should not pay for poor records management and longer review times caused by inexperienced access coordinators. Proponents also indicate that open and transparent governments should inform the public of its activities without fees.

There are also those who advocate for fees, arguing that fees should be charged so government can recover some of the cost of processing requests, and to encourage applicants to be reasonable in scope of requests.

The following information has been compiled from the *ATIPPA* Annual Report 2012-13 and from Office of the Information and Privacy Commissioner Annual Reports from 2008-09 to 2012-13.

Year	# of Access Requests (general and personal information)	Application Fees Collected	# of Requests Represented by Application Fees	# of Requests for General Access	Processing Fees Collected	Total Amount Collected (application fees and processing fees)	# of Requests Abandoned or Withdrawn	# of Complaints/Requests for review regarding fees received by OIPC
2012-13	660	2860.00	572	511	4663.95	7523.95	36	6
2011-12	537	2405.00	481	449	5551.82	7956.82	35	6
2010-11	566	2700.00	540	504	3964.75	6664.75	65	12
2009-10	547	2585.00	517	499	4172.82	6757.82	46	17
2008-09	493	2305.00	461	441	4617.54	6922.54	58	19

1 Newfoundland and Labrador Office of Public Engagement. *Access to Information and Protection of Privacy Act Annual Report 2012-13* http://www.atipp.gov.nl.ca/publications/ATIPPA_Annual-Report-2012-13.pdf

[2]2 Council of Europe Convention on *Access to Official Documents* (2009) http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=205&CM=1&CL=ENG

3 Centre for Law and Democracy. *Ireland: Campaign to block FOI fee increases successful, but unacceptable €15 up-front fee remains* (2011). http://www.law-democracy.org/live/ireland-campaign-to-block-foi-fee-increases-successful-but-unacceptable-e15-up-front-fee-remains/

4 Government of Canada. *Strengthening the Access to Information Act A Discussion of Ideas Intrinsic to the Reform of the Access to Information Act* (April 11, 2006): 31. http://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/atia-lai/atia-lai.pdf

5 Beeby, Dean. *Feds eye access-to-information fee hike to 'control demand'* published online at the Globe and Mail on March 13, 2011. http://www.theglobeandmail.com/news/politics/feds-eye-access-to-information-fee-hike-to-control-demand/article571747/

6 New Brunswick Department of Supply and Service. *Fees removed for right to information requests* (August 26, 2011). http://www2.gnb.ca/content/gnb/en/news/news_release.2011.08.0927.html

7 Department of Government Services *Right to Information Annual Report 2012-13* (May 2014): 2. http://www2.gnb.ca/content/dam/gnb/Departments/gs-sg/pdf/Publications/AnnualReport2012-2013.pdf

8 Office of Public Engagement. *Establishment of Fees and Forms for the Access to Information and Protection of Privacy Act* (December 10, 2012) http://www.atipp.gov.nl.ca/info/fees.pdf

9 Newfoundland and Labrador Office of Public Engagement http://www.atipp.gov.nl.ca/publications/ATIPPA_Annual-Report-2012-13.pdf

10 British Columbia *Freedom of Information and Protection of Privacy Act Freedom of Information and Protection of Privacy Regulation*(June 25. 2012). http://www.bclaws.ca/civix/document/id/complete/statreg/155_2012#section13

11 United States Department of State. *Information Access Guide* http://foia.state.gov/Request/Guide.aspx#FeesRequesterCategories

12 United States Department of Justice. *FOIA.GOV Frequently Asked Questions* http://www.foia.gov/faq.html#cost

13 Quebec *Regulation respecting fees for the transcription, reproduction or transmission of documents or personal information An Act respecting Access to documents held by public bodies and the Protection of personal information*

http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=3&file=/A_2_1/A2_1R3_A.HTM

14 Human Rights Committee, 102nd session, Geneva. *General Comment No.34: Article 19: Freedoms of opinion and expression* (July 2011) http://www.article19.org/resources.php/resource/2420/en/general-comment-no.34:-article-19:-freedoms-of-opinion-and-expression#sthash.hCvooJpK.dpuf 2011 General Comment on Article 19, para. 19

15 Centre for Law and Democracy. *Response to the OIC Call for Dialogue: Recommendations for Improving the Right to Information in* Canada (January 2013) www.law-http://www.law-democracy.org/live/wp-content/uploads/2013/01/Canada.RTI_.Jan13.pdf

16 Banisar, David. Freedom of Information Around the World 2006: A Global Survey of Access to Government Information Laws (2006) http://www.freedominfo.org/documents/global_survey2006.pdf

APPENDIX 2

ATIPPA Review 2014

Biological Samples

Introduction

In 2010-11, the Office of the Privacy Commissioner of Canada (OPC) funded a project called *Privacy in Canadian Paediatric Biobanks: A changing landscape* as part of their Contributions Program. One of the recommendations contained in the report was that the "OPC should specify in privacy legislation that genetic information and biological materials are considered personal health data." [i] The study found that, while privacy legislation prohibited the sharing of information derived from the biological sample without the individual's consent, the same did not apply to the biological sample itself. In addition, legislation provides a right of access to information derived from the sample, but not to the sample itself. As the focus of the study was on paediatric biobanks, it highlighted a variety of reasons why participants might want access to their samples in the future for testing, diagnosis or treatment purposes.

What is a Human Biological Sample?

The Tri-Council Policy Statement *Ethical Conduct for Research Involving Humans*, defines human biological materials as including "…tissues, organs, blood, plasma, skin, serum, DNA, RNA, proteins, cells, hair, nail clippings, urine, saliva and other body fluids."[ii] Biological samples contain a plethora of personal information, including ethnic percentages, geographic information, sex chromosomes and genetic predispositions to certain diseases, such as diabetes.[iii]

The Article 29 Data Protection Working Group, an independent advisory body on data protection and privacy, with members from the national data protection authorities of the European Union Member States, the European Data Protection Supervisor and the European Commission,[iv] noted that biometric data,

> *…may be defined as biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability… A particularity of biometric data is that they can be considered both as content of the information about a particular individual… as well as an element to establish a link between one piece of information and the individual.*[v]

During an appearance before the Standing Committee on Public Safety and National Security, a representative from the Privacy Commissioner of Canada's office noted that DNA data "…represents the intersection of both physical privacy and informational privacy interests."[vi]

As science advances, so too does the breadth and depth of information available from biological samples. As these advancements impact individual privacy, it is important to stay abreast of new developments and ensure the appropriate safeguards are in place.

Is a Human Biological Sample Identifiable Information?

The *Access to Information and Protection of Privacy Act (ATIPPA)* defines personal information as "recorded information about an identifiable individual."[vii] With regard to biological samples, this raises some interesting questions that have yet to be determined under *ATIPPA*. For example, an interpretation bulletin on personal information published on the Office of the Privacy Commissioner of Canada's website, has determined that "information need not be recorded for it to constitute personal information. It is sufficient that the information be about an identifiable individual even if the information is not in a recorded form, such as…biological samples…"[viii] However, the definition of personal information in *PIPEDA* and *ATIPPA* differs. *PIPEDA* defines personal information to mean "information about an identifiable individual", while *ATIPPA* defines it as "recorded information about an identifiable individual." As the *PIPEDA* interpretation bulletin used biological samples as an example of personal information in a non-recorded format, it would be difficult to include the sample itself as personal information under *ATIPPA*. That being said, if a biological sample containing a direct identifier, such as a label with a name or health number, was lost, this office would consider accepting a privacy complaint regarding the information rather than the sample itself under *ATIPPA* or *PHIA*.

Any information in oral or recorded form derived from the sample might be considered personal health information under the *Personal Health Information Act (PHIA)*, even in the absence of direct identifiers. *PHIA* defines personal health information as "identifying information in oral or recorded form about an individual that relates to …(c) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance."[ix]

A case heard before the Federal Court of Appeal, *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, examined the definition of personal information in the *Access to Information Act* when access requests for recordings and/or transcripts of air traffic control communications were denied based on the "personal information" exception. Madame Justice Desjardins, for the Court, determined that "…information recorded in any form is information "about" a particular individual if it "permits" or "leads" to the possible identification of the individual, whether alone or when combined with information from sources "otherwise available" including sources publicly available."[x] However, the Court also acknowledged the practice of the Supreme Court of Canada to read the *Access to Information Act* and the *Privacy Act* together as a "seamless code" following a "parallel interpretation model." Madame Justice Desjardins further notes that, when considering personal information in the context of the *Privacy Act:*

> *Privacy may be defined as an individual's right to determine for himself when, how and to what extent he will release personal information about himself. Privacy thus connotes concepts of intimacy, identity, dignity and integrity of the individual. The information at issue was not "about" an individual since the content of the communications did not involve subjects that engaged an individual's right to privacy. The information at issue was of a professional and non-personal nature. It could lead to identifying an individual and assist in determining how an individual performed his or her task in a given situation but did not qualify as personal information. It was not about an individual, considering that it did not match the concept of "privacy" and the values that concept was meant to protect.*

In the case of *Gordon v. Canada (Health),* heard before the Federal Court of Canada, both the *Privacy Act* and the *Access to Information Act* were cited when Health Canada withheld certain fields from a copy of the Canadian Adverse Drug Reactions Information System provided to the Applicant. The Court adopted a test suggested by the Counsel for the Privacy Commissioner, the Intervener, in determining when information is about an identifiable individual: "Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information." [xi] The Office of the Privacy Commissioner of Canada, in an interpretation bulletin regarding the definition of personal information in *PIPEDA*, notes that personal information that has been de-identified does not qualify as anonymous information if there is a serious possibility of linking the de-identified data back to an identifiable individual.[xii]

While some may argue that few individuals would have the capability and equipment to affiliate a biological sample with an identifiable individual, in *PIPEDA* Case #2009-018, the Assistant Privacy Commissioner of Canada discussed re-identification risk, determining that "It is not necessary…to demonstrate that someone would necessarily go to all lengths to actually do so."[xiii]

Do international laws specifically include biological samples in their definition of personal information?

Internationally, the Article 29 Data Protection Working Group has defined personal data to mean

> *… any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*[xiv]

The International Association of Privacy Professionals surveyed the definition of personal data across 36 data protection laws in 30 countries. Both Columbia and France include genetic data in their definition of personal data. In Columbia, personal data is classified into three sub-categories, one of which is private data that "concerns only the data owner, due to its reserved and intimate nature." In France, personal data is "any information which directly or indirectly allows the identification of an individual." Further research was conducted by Global Privacy and Security Law, who interpreted this to include DNA and digital fingerprints, among other things.[xv]

On October 16, 2003, the United Nations Educational, Scientific and Cultural Organization (UNESCO) made an International Declaration on Human Genetic Data. Article 14(b) of the declaration indicated that

> *Human genetic data, human proteomic data and biological samples linked to an identifiable person should not be disclosed or made accessible to third parties… except for an important public interest reason in cases restrictively provided for by domestic law consistent with the international law of human rights or where the prior, free, informed and express consent of the person concerned has been obtained provided that such consent is in accordance with domestic law and the international law of human rights.*[xvi]

Could there be a Valid Privacy Complaint Involving Biological Material Under *ATIPPA/ PHIA*?

The issue of how a privacy complaint regarding information derived from a biological sample would be addressed depends on the source of the information. The Tri-Council Policy Statement 2 discusses the sources of biological materials, including "patients following diagnostic or therapeutic procedures, autopsy specimens, donations of organs or tissue from living or dead humans, body wastes (including urine, saliva, sweat) or abandoned tissue. Biological materials may also be sought from individuals for use in a specific research project."[xvii] Additionally, biological samples may be collected for the purpose of law enforcement or for employment purposes.

The purpose of *PHIA* is to establish rules for the collection, use and disclosure of personal health information, including ensuring that appropriate safeguards are in place to protect the personal health information.

It is safe to assume that the majority of human biological samples collected in the province are collected by a health care professional or their designate for the primary purpose of the provision of health care. While a limited number of samples may be collected on behalf of employers for such purposes as screening to ensure compliance with contractual arrangements or treatment programs, the samples themselves would likely be collected by a health care professional. While the employer may be privy to certain information derived from the sample and may make employment or disciplinary decisions based on that information, the health care professional would likely be the custodian of the sample and any affiliated reports. As these samples would be affiliated with a particular individual, either through direct or indirect identifiers, they would be considered identifiable information and should be afforded appropriate safeguards by the custodian or information manager. *PHIA* would also address secondary use of any samples, such as for research purposes.

While these issues have yet to be decided under *PHIA*, it is difficult to argue that a biological sample itself is personal health information. Identifying information, such as a name or health care number, might be considered personal health information and a report on the information derived from the sample, even in the absence of direct identifiers, may be considered personal health information as well.

The purpose of *ATIPPA* is to make public bodies more accountable to the public and to protect personal privacy; one of the ways the Act does this is to restrict collection, use and disclosure of personal information. It should be noted that Section 5 of *ATIPPA* excludes certain records:

5. (1) This Act applies to all records in the custody of or under the control of a public body but does not apply to

> *(a) a record in a court file, a record of a judge of the Trial Division, Court of Appeal, or Provincial Court, a judicial administration record or a record relating to support services provided to the judges of those courts;*
> *(h) a record containing teaching materials or research information of an employee of a post-secondary educational institution;*
> *(k) a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed;*

(l) a record relating to an investigation by the Royal Newfoundland Constabulary if all matters in respect of the investigation have not been completed; or

(m) a record relating to an investigation by the Royal Newfoundland Constabulary that would reveal the identity of a confidential source of information or reveal information provided by that source with respect to a law enforcement matter.[xviii]

A biological sample taken for law enforcement and potentially by a researcher at a post-secondary institution may be excluded under *ATIPPA* even if biological samples were added to the definition of personal information. The information derived from the samples is currently excluded for the same reasons, to the extent described in Section 5.

Biological Samples and Law Enforcement

Under Section 487 of the Criminal Code of Canada, law enforcement is able to collect DNA samples and, for primary designated offenses, shall collect a sample for the national DNA Bank. The National DNA Databank was established by the *DNA Identification Act* and contains biological samples from convicted offenders and crime scenes. Law enforcement may ask judges to consider compelling a DNA sample for some secondary designated offenses as well.[xix] In the Government of Newfoundland and Labrador's *Public Prosecutions Guide Book*, it indicates that

Secondary discretionary or hybrid DNA offences require an application by the Crown to satisfy the sentencing judge that the DNA order is in the best interest of the administration of justice. Prosecutors should always consider whether a DNA order should be sought for secondary offences, and make the request in appropriate cases.[xx]

The Ontario Court of Appeal, in *R. v. Hendry,* recognized that "the taking and retention of a DNA sample constitutes a grave intrusion on a person's right to personal and informational privacy." The Court instructed that, when it comes to primary designated offenses, one must examine "whether the impact of a DNA order on an accused's privacy and security is grossly disproportionate to the public interest…" In addition, "the test is the same for both adults and young persons and a court cannot simply infer a disproportionate impact based on age alone."[xxi]

In general, law enforcement is able to obtain DNA samples using a warrant or through voluntary offerings by individuals. Legislation also exists for the Canadian forces, through the *National Defense Act* (section 196.11). The Criminal Code allows law enforcement officials to obtain a blood sample from an individual suspected of driving under the influence if the individual is unable to submit to other tests (section 254(3)(b)), if they have successfully applied for a warrant (section 256) or if they have successfully applied for a warrant to search and seize relevant evidence, including blood samples taken for treatment purposes (section 487).

Biological Samples and the Canadian Courts

In *R. v Dyment (1988),* the Supreme Court of Canada noted that health information and tissue "remain in a fundamental sense one's own."[xxii] In this case, a physician obtained a blood sample for the purpose of the provision of health care and provided it to police representatives without the patient's consent and without a request from the police. It was determined that "Receipt by the police of the vial of blood, given that that blood was held by the doctor subject to a duty to respect the

patient's privacy, amounted to a seizure as contemplated by s. 8 of the Charter ." The search was deemed unreasonable and it was further determined that Section 7 of the Charter – the right to life liberty and security of the person – had also been violated. The Court determined,

> *The seizure here infringed upon all the spheres of privacy -- spatial, physical and informational....As I see it, the essence of a seizure under s. 8 is the taking of a thing from a person by a public authority without that person's consent...The use of a person's body without his consent to obtain information about him invades an area of privacy essential to the maintenance of his human dignity.*[xxiii]

In its decision, the Court quoted the Report of the Task Force established by the Department of Communications/Department of Justice *Privacy and Computers*, "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit."

Access to Biological Samples

Should biological samples be added to the definition of personal information and/or personal health information, access rights to the sample itself should be considered. Access to biological samples by the individuals that provided them may not be absolute and, in fact, in some cases may not be possible. Even if access were be considered for the purpose of medical testing, diagnosis or treatment, the impact on the integrity of the sample itself must be considered (i.e. is it physically possible to provide part of the material, the impact that providing part of the sample will have on the remaining sample, and any related public health concerns).

While not specifically addressing biological samples, limits on access have been examined by the Courts. *McInerney v. MacDonald* provides guidance on a patient's right of access to their medical record. In this case, the Supreme Court of Canada ruled that "The patient is not entitled to the records themselves. The physical medical records of the patient belong to the physician." However, it also noted that, "In the absence of legislation, a patient is entitled, upon request, to examine and copy all information in her medical records which the physician considered in administering advice or treatment, including records prepared by other doctors that the physician may have received."[xxiv] In *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General),* Justice Deschamps noted, "...in a situation involving personal information about an individual, the right to privacy is paramount over the right of access to information."[xxv]

---

[i] Dove, Edward, Lee Black, Denise Avard and Bartha Knoppers. *Privacy in Canadian Paediatric Biobanks: A Changing Landscape* (2011): 62.
http://www.humgen.org/int/GI/Privacy_in_Canadian_paediatric_Biobanks.pdf

[ii] Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada,
and Social Sciences and Humanities Research Council of Canada. *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans* (December 2010): 169.
http://www.pre.ethics.gc.ca/pdf/eng/tcps2/TCPS_2_FINAL_Web.pdf

[iii] Family Tree DNA, https://www.familytreedna.com/

iv European Commission Justice. *Article 29 Working Party.* http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

v Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data*: 8. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[vi] Representative from the Privacy Commissioner of Canada (Lisa Madelon Campbell, Acting General Counsel). *Appearance before the Standing Committee on Public Safety and National Security* (February 26, 2009). https://www.priv.gc.ca/parl/2009/parl_090226_lc_e.asp

[vii] *Access to Information and Protection of Privacy Act*, S.N.L. 2002. http://assembly.nl.ca/Legislation/sr/statutes/a01-1.htm

[viii] Privacy Commissioner of Canada.

[ix] *Personal Health Information Act*, S.N.L. 2008. http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm

[x] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)* (F.C.A.), 2006 FCA 157, [2007] 1 F.C.R. 203. http://reports.fja-cmf.gc.ca/eng/2007/2006fca157.html

[xi] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*

[xii] Privacy Commissioner of Canada. *PIPEDA Personal Information Interpretation Bulletin.* https://www.priv.gc.ca/leg_c/interpretations_02_e.asp

[xiii] Privacy Commissioner of Canada. *PIPEDA Case Summary #2009-018 (2009).* https://www.priv.gc.ca/cf-dc/2009/2009_018_0223_e.asp

[xiv] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 *on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (1995). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[xv] Baker, William and Anthony Matyjaszewski. *The Changing meaning of personal data* (2010). https://privacyassociation.org/resources/article/the-changing-meaning-of-personal-data/

[xvi] United Nations Educational, Scientific and Cultural Organization (UNESCO). *International Declaration on Human Genetic Data* (2003) http://portal.unesco.org/en/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html

[xvii] Canadian Institutes of Health Research et al.

[xviii] *ATIPPA*

[xix] Royal Canadian Mounted Police. *National DNA Databank.* http://www.rcmp-grc.gc.ca/nddb-bndg/index-accueil-eng.htm

[xx] Office of the Director of Public Prosecutions. *Guide Book of Policies and Procedures for the Conduct of Criminal Prosecutions in Newfoundland and Labrador* (October 2007). http://www.justice.gov.nl.ca/just/prosect/guidebook/012A.pdf

[xxi] *R. v. Hendry (2001) 161 C.C.C. (3d) 275* http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/2242/index.do

[xxii] *R. v.Dyment*, [1988] 2 S.C.R. 417. http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/375/index.do

[xxiii] *R. v.Dyment*

[xxiv] *McInerneyv. MacDonald*, [1992] 2 S.C.R. 138. http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/884/index.do

[xxv] *H.J. Heinz Co. of Canada Ltd. v. Canada (Attorney General)*, [2006] 1 S.C.R. 441, 2006 SCC 13, http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/8/index.do

OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

APPENDIX 3

January 22, 2013

Honourable Joan Shea
Minister
Department of Advanced Education and Skills
P.O. Box 8700
Confederation Building
St. John's, NL
A1B 4J6

Dear Minister Shea:

Subject: Privacy Complaint under the *Access to Information and Protection of Privacy Act*
Our File: 0035-094-12-001

The Office of the Information and Privacy Commissioner ("the OIPC") received a Complaint from Gerry Rogers, MHA for St. John's Centre dated August 14, 2012 regarding the policy or practice that requires MHAs to contact a Minister's Executive Assistant if the MHA is making an inquiry on behalf of a constituent. As you are aware, this Office has undertaken an investigation with respect to the Complaint under the *Access to Information and Protection of Privacy Act* (the "*ATIPPA*"). Ms. Rogers' letter raised a number of issues with this policy or practice, however, the OIPC has limited the scope of its inquiry to issues relating to privacy within the jurisdiction of this Office. The OIPC received your reply to this complaint dated October 17, 2012.

With respect to the issue of requiring a consent form signed by the constituent authorizing an MHA or their staff to access the constituent's personal information, the OIPC supports and endorses this practice. While Section 5.10.7 (Disclosure to a Member of the House of Assembly) permits release of information by a public body employee to an MHA (or designated constituency assistant) with the verbal consent of the constituent, the OIPC is of the belief that written consent is preferable in circumstances where it can reasonably be obtained. The OIPC recommends the use of written consent, with the caveat that in exceptional circumstances where obtaining written consent (i.e. timeliness, urgency, etc.) is difficult and may compromise the assistance of the MHA, verbal consent should be acceptable.

With respect to the "new policy" of requiring MHAs to direct requests for information pertaining to a constituent through a Ministerial Executive Assistant, we were advised further to our inquiry on this matter that no formal written policy exists. It is the finding of the OIPC that there has been some sort of informal practice or procedure in place since 2003 and that the continuation of this procedure was reinforced verbally to public service staff as recently as this year. It is not clear whether this procedure was generally followed in the past, nor is it clear whether all departments are enforcing this procedure. Further, it is not clear to the OIPC whether in all circumstances the

department in question (Advanced Education and Skills) is consistently implementing this practice or not. The lack of a written policy and therefore lack of records on the subject matter of this complaint challenges the ability of the OPIC to comment definitively on the privacy implications of this practice/procedure under the *ATIPPA*.

That being said, the OIPC does have concerns regarding this practice or procedure which require clarification. Clearly, the *ATIPPA* is meant to facilitate the work of MHAs through section 30(1)(k), which allows a public body to disclose personal information "to a member of the House of Assembly who has been requested by the individual the information is about to assist in resolving a problem." It is important to recognize that the constituent has asked the MHA for assistance, and there is provision in section 30(1)(k) for the constituent's information, as it pertains to the issue at hand, to be disclosed to the MHA in order to allow the MHA to provide that assistance. The constituent has a reasonable expectation that the process of providing the information necessary to assist in addressing his or her problem will not result in the information being funneled through additional channels which may result in more people than necessary becoming aware of the personal information of the constituent. In this regard, section 38(2) of the *ATIPPA* is relevant:

> *38(2) The use of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.*

The practice or unwritten policy directing MHAs to make such inquiries through the Ministerial Executive Assistant may, in certain cases, be consistent with the *ATIPPA*, however. Inquiries which involve elements such as the exercise of discretion at a senior or Ministerial level may be more suitably directed to an official in the Minister's Office. Furthermore, inquiries which are focused on divergent interpretation of policy which require interpretation by senior officials may also be more appropriately addressed to the Minister's Office. Essentially, complicated or unusual inquiries may meet the threshold set out in section 38(2), which is to say that the use or disclosure of information to an official in the Minister's Office, or even the Minister or other appropriate staff, are dictated by the circumstances of the request itself. In the language of section 38(2), it may in fact be *necessary* to work directly with staff in the Minister's Office in order for the MHA to proceed with his or her inquiry on behalf of the constituent.

On the other hand, there is no apparent basis in the *ATIPPA* for providing the personal information of constituents to individuals within the Minister's Office when the inquiry is of a more routine nature. When such information is shared with or provided to persons within a public body beyond that which is "necessary" to accomplish the purpose, this use of personal information is not compliant with section 38(2) of the *ATIPPA*. Particularly when written consent has been provided by the constituent (as discussed above) for the MHA to make inquiries on their behalf and to receive information relevant to the issue they have been asked to assist with, there would seem to be very little basis in the *ATIPPA* to require that such an inquiry be simply passed along by the MHA to an individual in the Minister's Office who is not directly involved in the matter, but who is then expected to make inquiries directly to staff and report back the MHA. Certainly, I see no basis to argue that such a process would be a "necessary" use of personal information as contemplated by section 38(2).

In summary, I conclude that on its face, a policy of requiring certain types of more complex inquiries to be routed through the Minister's Executive Assistant would not contravene the *ATIPPA*, however applying the same requirement to routine inquiries by MHAs on behalf of

citizens would appear to insert an unnecessary third party (the Executive Assistant) into the process. One final point to note would be that my comments should not be interpreted to mean that every public servant is obliged to deal directly with an MHA inquiry. If a front line worker and a manager are both privy to a file involving a constituent who has requested his or her MHA to provide assistance and make inquiries on his or her behalf, it is within the discretion of the Department to determine which of these individuals at the level of service is most well placed to respond to the inquiry.

The OIPC recommends that if the Department wishes to continue using this practice, a formal policy should be drafted which could outline to both MHAs and departmental staff what is expected in such situations, with special emphasis on limiting any unnecessary sharing or use of the identity of the constituent where possible, and limiting the number of individuals who are viewing the personal information to those who are necessary to the process of responding to the constituent's request for assistance to his or her MHA. Furthermore, the OIPC is available to review or provide consultation on the privacy implications of any such draft policy at your request. We ask that you respond to this letter and recommendation within 30 days.

Yours truly,

Rodney S. Hynes
Research and Policy Development Specialist

cc. Ms. Gerry Rogers, MHA