SUBMISSIONS OF THE INFORMATION AND PRIVACY COMMISSIONER

BILL 29—AN ACT TO AMEND THE ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT

January 2019

TABLE OF CONTENTS

INTRODUCTION

This submission offers my comments on Bill 29, which would amend the *Access to Information and Protection of Privacy Act* (Act).

Many of the proposed amendments are very positive and I strongly support them. Some of the amendments are, however, less constructive and my concerns about them are expressed below, arranged by theme and topic.

Similarly, I am concerned that the amendments would not respond to some of the issues raised in my October 2015 submission in response to the government's consultation on possible amendments to the Act.[1]

Accordingly, while I commend the government for its commitment to improving the Act through Bill 29, I urge the government to introduce amendments to Bill 29 in light of this submission.

This document first sets out my submissions on Bill 29, while the second part discusses amendments that are not found in Bill 29 but which, in my view, are vital to ensuring that the amendments are as current as they can be to meet the needs of today's business realities.

I look forward to appearing before the committee to elaborate on the observations in this submission and to assist the House with Bill 29.

January 2019

Elaine Keenan Bengts
Information and Privacy Commissioner

[1] *Submissions of the Information and Privacy Commissioner on the Comprehensive Review of the Access to Information and Protection of Privacy Act* (October 13, 2015), referred to below as the "2015 submission" and found here: https://atipp-nt.ca/wp-content/uploads/2018/08/Comprehensive-Review-Submissions.pdf.

1.0 COMMENTS ON BILL 29'S AMENDMENTS

This section discusses the proposed amendments that would affect the Act's scope and coverage. It also discusses amendments to the Act that should be addressed in Bill 29.

1.1 COVERAGE OF MUNICIPALITIES

Local governments provide vitally-important services to residents and have a direct impact on their day-to-day life. The well-accepted policy of transparency and accountability underlying the Act should apply to local governments. In this light, a very positive aspect of Bill 29 is that it will enable municipalities to be designated by regulation as public bodies under the Act.[2] This is a welcome step.

I urge the government to consult with my office regarding which municipalities are to be designated as public bodies. I would hope that the larger municipalities such as Hay River, Inuvik, Fort Smith, and especially Yellowknife, would be designated at an early date.

Section 10 of Bill 29 would add a new section 13.1, which would protect certain municipal confidences. It would protect draft bylaws and resolutions and the substance of *in camera* deliberations of municipal councils and their committees. The new provision is acceptable, noting that it aligns well with similar protections in other access laws, including Ontario, Alberta and British Columbia.

1.2 EXCLUSION OF CONSTITUENCY RECORDS

Section 3 of Bill 29 would exclude from the right of access any "personal or constituency record" of a member of the Legislative Assembly that is in the custody or control of the member, the Legislative Assembly or a public body. It would also exclude such records of a member of a municipality. As stated in my 2015 submission, I see no reason for either exclusion. My office has not had matters of this kind come before it and the existing concepts of "custody" and "control" under the Act can easily deal with such issues if they arise.[3] Introducing the new concepts of "personal" or "constituency" records, which are not defined, is not necessary and could create confusion.

[2] Bill 29 would amend section 2 of the Act to provide that a "public body" covered under the Act includes any municipality under the *Cities, Towns and Villages Act*, the *Charter Communities Act* or the *Hamlets Act* that is designated as a public body by regulation.
[3] 2015 submission, pages 5-6.

1.3 PUBLIC INTEREST OVERRIDE

My 2015 submission called for introduction of a requirement that to disclose information the disclosure of which is in the public interest, despite any of the Act's disclosure exemptions.[4] The proposed amendments include a form of public interest override. The proposal does not go far enough by a long stretch in terms of which exemptions it would override. It also inappropriately places a burden on access applicants to demonstrate that there is a public interest in disclosure of information that, by definition, they know nothing about.

The override proposed in a new section 5.1 would prevail over only four of the Act's many disclosure exemptions: advice from officials (section 14), intergovernmental relations (section 16), economic interests of the government (section 17), and harm to another individual or the applicant (section 21). By contrast, the public interest overrides in the British Columbia *Freedom of Information and Protection of Privacy Act* and the Alberta *Freedom of Information and Protection of Privacy Act* prevail over all of the secrecy provisions in those laws where disclosure is "clearly in the public interest".[5] Those laws also add a second public interest consideration, by requiring disclosure of information where it is about a risk to health or safety or to the environment.

Starting with the latter public interest test, risk of harm to the environment or human health or safety is surely paramount to considerations of business or government secrecy. So is protection of the environment. What if, for example, the government possesses information showing that a particular business is polluting the environment and that this creates a serious risk of harm to human health or safety? Surely the business's interests should not prevail over the health or safety of communities or groups of people? There needs to be a public interest override in such cases.

Therefore, Bill 29 should be amended to provide that a public body is required to disclose to the public, an affected group of people or an applicant, as promptly as practicable, information about a risk of serious harm to the environment or to the health or safety of the public or a group of people. This duty should apply, to be clear, regardless of whether an access request has been made.

Beyond cases of risk of harm to health or safety or the environment, public interest disclosure should be required where the public interest otherwise favours it. This is the approach in other

[4] 2015 submission, pages 2-3.

[5] Sections 25(1) of the British Columbia *Freedom of Information and Protection of Privacy Act* [BC FIPPA] and section 32(1) of the Alberta *Freedom of Information and Protection of Privacy Act* [Alberta FIPPA].

jurisdictions, including Ontario, Alberta and British Columbia. The Ontario threshold requires a "compelling" public interest in disclosure.

Another significant concern is that the amendment would trigger disclosure only where a "compelling" public interest "clearly outweighs the purpose of the exemption". Requiring there to be a "compelling" public interest that "clearly outweighs" the goal of each exemption that might apply imposes an inordinately high bar. Experience in Ontario with similar language shows that the bar is so high that the override will effectively be illusory. The proposed public interest override will, given this unnecessarily onerous text, effectively gut itself in practice.

By contrast to Ontario, both Alberta and British Columbia have set a threshold that requires disclosure where it is "clearly in the public interest".[6] This is, in my view, more consistent with the important public policy goals of access to information legislation. In that spirit, I believe the Act should require a public body to disclose information where the public interest in disclosure "clearly outweighs" the policy objectives underlying the access exemptions that would otherwise apply and permit the information to be kept secret. This is the approach taken in Newfoundland and Labrador, an approach I have previously endorsed.[7]

It is also desirable for the public interest override to override *all* of the Act's provisions, as is the case in Alberta and British Columbia, not just a select few. If disclosure of information is truly in the public interest it should override all other considerations, and thus all of the Act's access exemptions. In this regard, it is useful to recall the policy goals of access to information as they reflect the public interest:

> [I]n a modern law and one that reflects leading practices in Canada and internationally, it is necessary to broaden the public interest override and have it apply to most discretionary exemptions. This would require officials to balance the potential for harm associated with releasing information on an access request against the public interest in preserving fundamental democratic and political values. These include values such as good governance, including transparency and accountability; the health of the democratic process; the upholding of justice; ensuring the honesty of public officials; general good decision making by public officials. Restricting the public interest to the current narrow list implies that these other matters are less important.[8]

[6] BC FIPPA, section 25(1)(b).
[7] This recommendation is set out in the 2015 submission, which adopts the recommendation of the Report of the 2014 Statutory Review of the *Access to Information and Protection of Privacy Act* (Queen's Printer, Newfoundland and Labrador, 2014) [Newfoundland report], at page 79.
[8] Newfoundland report, at page 78.

As noted earlier, the Bill 29 approach would only override four of the Act's exemptions, leaving a number of other exemptions to apply even though they could, in a meritorious case, needlessly stymy disclosure in the public interest. The fact that a public body might, in a given case, waive a discretionary exemption and disclose information is not an answer to this concern. However, if Bill 29 is not amended so that all exemptions can be overridden, the list of exemptions that can be overridden should be expanded.

At present Bill 29 would permit the public interest to override only four exemptions, as noted above. A notable omission from the list is section 24 of the Act, which protects certain third-party business interests. It is entirely plausible to think of a situation where business information that may be protected under section 24 reveals an environmental or public health threat and thus ought to be disclosed in the public interest. The example of pollution data comes to mind. In fact, such a case recently arose in British Columbia, with the Information and Privacy Commissioner of British Columbia requiring the government to release the results of water testing that had found pollution of local water tables due to activities on privately-owned land.[9] Section 24 therefore should be added to the list of exemptions in section 4 of Bill 29. Section 18, which protects the results of tests or audits, should also be added for the same reasons.

A similar argument exists for Cabinet confidences. The protection for Cabinet-related materials, found in section 13 of the Act is very broad and could exempt materials the disclosure of which is clearly in the public interest. The point is that, at common law, the public interest immunity principle that protects Cabinet confidences is not absolute in the first place. The Supreme Court of Canada has affirmed more than once that "the public interest in Cabinet confidences must be balanced against the public interest in disclosure, to which it might sometimes be required to yield".[10] However, this balancing test applies only in litigation and is not available under the Act. Extending the public interest override under the Act to Cabinet confidences would provide that necessary mechanism. Section 13 should be added to the list of exemptions listed in section 4 of Bill 29.

Two other features of the new section 5.1 proposed under Bill 29 raise concerns.

First, unlike Ontario, British Columbia or Alberta, section 5.1 would explicitly place the burden on an access applicant to prove, to "demonstrate", that that the public interest compellingly favours disclosure of the information. Applicants will, by definition, not know what is in the

[9] Investigation Report F16-02: https://www.oipc.bc.ca/investigation-reports/1972.
[10] *Babcock v. Canada (Attorney General)*, 2002 SCC 57, at paragraph 19.

records they have asked for and their knowledge of surrounding circumstances often will be incomplete.

Put another way, applicants will in almost all cases be in the dark yet be expected to legally "demonstrate", from a position of complete or near-complete ignorance, how there is a "compelling" public interest in disclosure of the hidden information. This places an unacceptable burden on individual applicants and would all but completely gut the override. This feature of the amendment is out of line with public interest overrides in other Canadian jurisdictions. Bill 29 should not impose any burden on access applicants to "demonstrate" a public interest in disclosure. Public bodies should have the responsibility for determining, in each case, whether the public interest favours disclosure of information.

Second, section 5.1 should require a public body to consider whether disclosure is in the public interest even if an access request has not been made for the information in question. At present, section 5.1 would only be triggered if someone happens to make an access request for the information. This leaves protection of the public interest to chance. If disclosure is in the public interest, surely it should be mandatory? If a public body is aware of information about a serious risk of harm, or information the disclosure otherwise might be in the public interest, the public body should be required to consider whether release is required and to act on that basis. This would more fully respect the vitally-important public policy goals of access legislation as outlined above. It would also better serve other important public policy goals.

1.4 CHANGES TO DISCLOSURE EXEMPTIONS

Bill 29 would amend some access exemptions under the Act and my comments follow. If I have not commented below on a Bill 29 amendment, it means I support the amendment.

Cabinet confidences—Section 9 of Bill 29 would replace section 13, of the Act, which protects Executive Council confidences. It would include a definition of "Executive Council record". With two notable exceptions that definition, which would closely mirror the existing section 13, is supportable. The first concern is inclusion, through a new section 13(1)(g), of protection for any "record created during the process of developing or preparing a submission for the Executive Council or Financial Management Board". No guidance is offered on the nature or limits of the meaning of the term "process" for developing such submissions. At its extreme, it could sweep all aspects of public service communications that in any way were "created during" whatever ill-defined "process" is involved. This could include records that actually contain no policy, any advice or any recommendations. As long as a record was "created during" an ill-defined "process" that record would have to be protected (section 13 is mandatory: it cannot be

waived). The proposed section 13(1)(g) should be removed (or, perhaps, clarified and restricted in scope).

The second concern with the proposed section 13 is that a new section 13(1)(h) would *require* the government to refuse to disclose "that portion of a record which contains information about the contents of a record" otherwise protected under section 13. This is very broad and conceivably could, noting government's increasing use of electronic records, include metadata. Metadata are data about data. Metadata can convey information about how other data—here, the contents of an "Executive Council record"—were created, when the record was created, who created it, on which computer the record was created, the size of the records and how it was processed.

Knowing when a record was created, who created it and where it was created can be valuable information, without affecting the public policy goals of section 13, since none of this information is likely to reveal, directly or indirectly, the substantive content of an Executive Council record. Yet knowledge of this information could be valuable in achieving the accountability and transparency goals of the Act. As an example, this information could reveal that a business seeking a favourable legislative change submitted a fully-fledged legislative submission, including draft legislation, to the Executive Council. This would not disclose the contents of the submission, just the fact that it was made and by whom. This knowledge could be important in holding government to account for the outsourcing of public policy to private interests. Section 13(1)(h) should not be enacted.

Municipal confidences—As noted above, I support the proposed section 13.1, which would protect certain municipal government confidences.

Advice from officials—I strongly support section 11 of Bill 29, which would amend section 14(1) of the Act, to eliminate sections 14(1)(b) and (f). Section 14 protects advice, recommendations and other work product of public servants. Section 14(1)(b) permits the government to withhold "consultations or deliberations involving" public servants, members of Cabinet or Cabinet staff members. This provision as currently written has been used in many circumstances in an attempt to avoid the disclosure of records which, for whatever reason, might be embarrassing if disclosed or which a public body simply does not want to disclose for some reason. The current language is so vague as to be open to abuse so its elimination is a very positive step.

Elimination of section 14(1)(f) is welcome for the same reasons. It permits an agency, board, commission, corporation, office or other public body to withhold the "contents of agendas or

minutes of meetings" of that public body. Regardless of whether a meeting agenda or minutes contain any advice or recommendations, or other information meriting protection, a public body can now refuse disclosure altogether. This can leave the public in the dark about what is going on inside a public body in the ordinary course with no counterbalancing public interest benefit to this secrecy. If agendas or minutes contain information that should be protected, other aspects of section 14, and other exemptions under the Act, are available to do so. I strongly support this amendment.

Confidential employment evaluations—I am deeply concerned about the proposed new section 22(2) of the Act.[11] That provision would authorize a public body to refuse to disclose personal information that could reasonably identify "a participant in a formal employee evaluation process about the applicant" where that information is supplied in confidence. As the new section 22(3) suggests, this appears to be aimed at protecting formal peer review processes, where colleagues evaluate each other's job performance, but this is not entirely clear. Even if that is the intent, I am concerned that this amendment would inappropriately privilege the interests of anonymous commentators over the interests of individuals to know what is being said about them, true or not. There is no clear public interest case for this amendment, no plausible need to so dramatically up-end the balance between an employer's interest in proper evaluations and an individual's right to be protected against inaccurate or malicious comments.

An individual's right of access to her or his own personal information is of fundamental importance. This remains the case where co-workers are evaluating a colleague's performance. Even where a "formal employee evaluation process" is involved, there can be a real risk of unfounded or malicious evaluations. Statutory anonymity for those who provide inaccurate or wilfully false information would, perversely, be an incentive for carelessness or worse. Yet ill-informed or malicious comments can cost an employee possible future job promotions, or future career prospects elsewhere. These are, to say the least, significant consequences.

Each employee therefore should continue to have the right to know who has said what about them, in order to be able to counter false or inaccurate statements (or to add, knowing the context, his or her perspective on the statements). I recognize that this new section would only prevent disclosure of information that could reasonably identify the evaluator, not the evaluations themselves. However, especially in small workplaces, this undoubtedly could prevent employees from having access to the evaluation itself. Individuals who assess others should be prepared to stand behind what they say. This amendment should not proceed.

[11] This would be added by section 14 of Bill 29.

Exclusion of information about a "labour relations matter" or "workplace investigations"— Bill 29 would enact two new exclusions from the right of access under the Act. Like the proposed section 22(2), section 24.1 would drastically affect the current balance between privacy and transparency in this area.

It would require a public body to refuse to disclose "labour relations information" the disclosure of which could reasonably be expected to reveal any information whatsoever that has been supplied to, or the report of, an arbitrator, mediator, labour relations officer or other person or body appointed to resolve or inquire into a "labour relations matter". This would be a mandatory exemption, and a public body would not be permitted to waive its protection.

This is a potentially vast black hole in the Act. For one thing, the terms "labour relations information" and "labour relations matter" are not defined. They could be very broad in their scope. If these exemptions are enacted, my office will be required to give them some meaning through case-by-case adjudication. The preferred route is to define both of these terms in the Act and to define them narrowly.

I am also concerned, regarding the proposed section 24.1, that it would require public bodies to withhold even the final report of a labour arbitrator or similar decision-maker. It is not an answer to say that arbitration decisions are often published. This is by convention and in any case there is no good reason for an access to information law to require them to be secret. These decisions are an important part of our law and the Act should not require them to remain that way when an access request is made for unpublished decisions.

Business information of a third party—Bill 29 would enact a new version of section 24(1) of the Act. I support the new version of section 24(1)(a), which would clarify what kinds of third-party information may be protected under section 24(1). However, I do have concerns about other aspects of section 24.

I refer here to existing aspects of that exemption that would be continued through the new section 24, namely, the mandatory exemption of the following: amounts billed by a public body to a third party (new section 24(1)(c)); the amount of financial assistance provided to a third party by a "prescribed corporation or board" (new section 24(1)(d)); and information supplied by a third party in support of an application for financial assistance from a prescribed corporation or board (new section 24(1)(e)). Bill 29 presents an opportunity to remove these provisions and enhance public body accountability and I strongly believe they should be removed now.

These three exemptions are class exemptions: they authorize a public body to keep information secret as long as it falls within the described class. There is no need for the public body to show harm to its interests through disclosure or that disclosure would cause harm to someone else. At the same time, these exemptions shield possibly important information from public scrutiny.

It is not clear, for example, why a public body should not disclose financial information about the amounts it charges to a third party for "routine services" (whatever that vague term means). If disclosure in a given case could harm the public body, then it could rely on section 17(1). There is no reason for the broad blanket exemption, regardless of any possible harm, in section 24(1)(c).

The same argument applies to what will become sections 24(1)(d) and (e). In principle, if a "prescribed corporation or board" is giving public funds to a "third party" there is a strong public interest in knowing how much is being given at public expense. This is the case whether the third party is a public or private sector entity. Similarly, if a third party is seeking financial assistance from public funds, there is a strong argument for transparency around the information it supplies in support. If there is concern about harm to the third party's interests, section 24(1)(a) can protect the third party where there is evidence that disclosure of the information would cause harm. There is no reason to have the added blanket, class-based, exemption in section 24(1)(e).

There is no public policy reason to retain any of these class-based exemptions, including because any concerns about harm to a public body are very well dealt with through section 17 of the Act. Bill 29 should be amended to repeal sections 24(1)(c), (d) and (e).

1.5 PROCESS-RELATED & OTHER AMENDMENTS

Bill 29 would implement a number of changes to request-processing procedures under the Act. My comments on these proposed changes follow.

Business, not calendar, days—Section 5 of Bill 29 would substitute business days for calendar days in calculating time under the Act. Since a "business day" will exclude a Saturday, Sunday and statutory holiday, times under the Act will be calculated differently. This is not, in my view, of concern when it comes to access request response times. At present, section 8 of the Act requires public bodies to access requests within 30 calendar days after receipt. Bill 29 would change that to 20 business days. In practice, however, this amounts to roughly the same time period, one month.

Time extensions—Section 6 of Bill 29 would amend section 8 of the Act, to limit the ability of a public body to extend its time for responding to an access request, by imposing a 20-business day limit on initial extensions. This is a welcome change.

Also welcome is the new section 11.1, which would give the Information and Privacy Commissioner the authority to grant a further time extension. Requests can be complex and can involve a large number of records. They may also require consultation with other governments, agencies or individuals before an appropriate decision can be made. The new time limit on initial extensions and the ability for the Information and Privacy Commissioner to further extend the response time are consistent with my 2015 recommendations and are very welcome.[12]

However, I am concerned that the 20-day time limit on initial extensions taken by public bodies would not work if the third-party response time remains at 30 business days, as Bill 29 proposes. As noted below, Bill 29 would give third parties 30 business days to respond to a consultation notice. This means that, even if a public body extended the response time on the very day an access request is received, the extension by 20 business days would be too short to accommodate the 30 business days that the third party has to respond. As noted below, the third-party response period for consultations should be reduced to at most 15 business days, not 30. A 15-day consultation period would give public bodies five business days to make a decision after hearing from third parties, but this is the only way the 20 business days proposed in Bill 29 could work.

Another solution for this concern could be to add a new provision to the Act, to specifically deal with extensions where a public body has triggered a third-party consultation. Under this approach, the Bill 29-amended section 11 would authorize an initial 20-business day extension, but if a third party has been notified under section 26, a new provision would say something to the effect of, "where a public body has notified a third party pursuant to section 26 of the Act, the public body may extend the time for responding to a request for information for a period not exceeding "x" business days".

Transferring access requests—I also welcome section 8(1) of Bill 29, which would amend section 12(1), to require a public body that seeks to transfer a request to another body to do so within 10 business days after it receives the request. These amendments are consistent with my 2015 submission and will help ensure prompt transfers of requests to those who should properly reply.[13]

[12] 2015 submission, pages 15-16.
[13] 2015 submission, pages 15-16.

Consultations with third parties—Bill 29 offers the opportunity to fix concerns about the third-party consultation process under section 26 of the Act. Section 26 of the Act requires a public body to give notice to third parties in certain cases. The first is where the public body is considering disclosing personal information that may be protected under section 23; the second is where it is considering disclosure of business information that may be protected under section 24.[14] Bill 29 would somewhat shorten some of the timelines for third-party consultations, but it should reduce them further, as even the amended timelines will entail unnecessary delay in access requests.

Section 20 of Bill 29 would amend section 26 of the Act, to reduce the time for a third party to respond to a consultation notice from 60 days to 30 business days. This still gives third parties some six weeks to respond, which is still excessively generous. The response time in the comparable BC FIPPA provision is 20 business days;[15] in Ontario the response time is 20 calendar days.[16] There is no good reason for third parties to have six weeks to respond, while the impact on timely access requests is plain. Section 26 should, rather, be amended to give third parties 15 business days, or roughly three weeks, to respond. At the highest, it should give them 20 business days. Thirty business days is too long.

Similar changes are needed for the time a public body has to make its decision after it has heard from third parties. Bill 29 would amend section 27 of the Act to reduce the 30 calendar days for a public body to make a decision after hearing from third parties to 15 business days. In other words, this reduces the post-representation response time from roughly one month to approximately three weeks. There is no good reason for a public body to have up to three weeks to decide such matters. The post-representation timelines in the British Columbia and Ontario statutes are 10 business days[17] and 10 calendar days.[18] The timeline under our Act should not exceed 10 business days.

I will also note here, in passing, my concern about the timing of public body notifications under section 26. My office often encounters cases in which a public body has waited until the last possible moment before its 30-day access request deadline has expired before it gives third-party notice. This will inevitably add to delay in response to the access request. This is not

[14] The third party is then entitled to make written representations explaining why the information should not be disclosed or to consent to its disclosure. The public body is not bound by written representations but considers them in deciding whether to disclose the requested records.
[15] BC FIPPA, section 23(3)(c).
[16] *Freedom of Information and Protection of Privacy Act* (Ontario) [ON FIPPA], section 28(5).
[17] BC FIPPA, section 24(1).
[18] ON FIPPA, section 28(4).

something that can be fixed through the Act. I do, however, urge all public bodies to give third-party notice as soon as practicable during the 30-day response period.

Another recommendation relates to the practice of many public bodies to consult third parties even where they are not required to do so under section 26, *i.e.*, even where there is no third-party personal information or business information involved. The Act does not prevent this from happening and I acknowledge that consultations may help improve decisions, by providing contextual information to the public body. Nonetheless, I urge public bodies to conduct such informal consultations only where absolutely necessary, *e.g.*, where the information may be protected under section 16(1) (intergovernmental relations) or section 20 (prejudice to a law enforcement matter).

Processing of access reviews—I am deeply concerned about the change proposed by section 22 of Bill 29, which could have a drastic impact on my office's work. This provision would amend section 31(3) of the Act to reduce the time limit for my office to review public body access decisions. It would significantly decrease the time we have to do our work thoroughly and carefully, from 180 calendar days (roughly six months) to 60 business days (roughly three months).

The reason for this drastic step is not at all clear. Certainly, our caseloads are already such that, with current resources, we are not able to keep up with demand in as timely a fashion as I would like or that the public can expect. Imposition of such a severe constraint without my office having more resources would either cause my office to fail to meet that standard or, in order to do so, to divert scarce resources from other important tasks, such as privacy complaints under the *Health Information Act*. Neither outcome is desirable.

There is, in any case, a good case for eliminating the time limit altogether. My office's review functions differ from the work of public bodies when they decide whether or not to disclose information. They base such decisions on analysis of their own records and of contextual information that they possess.[19] By contrast, my office is utterly dependant on public bodies to be timely in responding to our requests for information when we receive an applicant's request for review.

We frequently encounter delays on the part of public bodies in providing us with copies of the records in dispute and in providing other information to assist our review. These delays are

[19] Third-party consultations are an exception to this, I acknowledge, requiring public bodies to rely on third parties to respond in a timely way and provide relevant information. As discussed above, however, this reliance on third parties is conditioned by the Act's express timelines for third-party responses.

often not deliberate, being due, rather, to lack of resources or other understandable factors. But the fact remains that we are often at the mercy of events outside or control, making it difficult for us to meet the existing 180-day timeline much less one half as long, as proposed.

Further, in a review the commissioner decides all questions of fact and law, *i.e.*, a review is a legal process requiring evidence, consideration of precedents, review of records and careful decision-making efforts. This is a time-consuming process in principle. As a practical matter, access to information disputes can be complex and very detailed, often with large volumes of records to review, often on a page-by-page, line-by-line basis. For these reasons, reviews are not quick and easy matters. They take time. Cutting my office's timelines for these matters by such a drastic amount would not be practical and would not recognize the efforts required to complete reviews.

In recognition of this, Bill 29 should not cut my office's response time in half. It should remain as it is, expressed of course in business days. Regardless, section 31 should also be amended to permit the commissioner to extend the review period, by notice to the parties, giving an anticipated date for completion. This is the approach in Alberta and Ontario imposes no time limits at all on its commissioner.[20]

New offences and fines—Bill 29 would amend section 59(2) in ways that I strongly support. Significantly, it would create a new offence of wilfully destroying records to evade an access request. It would also create a new offence of attempting to gain access to, or gaining access to, personal information for which the person has no authority to do so. Both of these will significantly enhance access and privacy rights. Similarly, the new maximum fine of $10,000.00 for each offence. These changes are commendable.

[20] Under section 69(6) of AB FIPPA, the commissioner may extend the period by notice, and must give an anticipated completion date when doing so. There is no maximum on the extension period. If, despite the above submission, a time limit is to remain for my office to complete a review, the authority to extend should be "for a reasonable period" or for successive extensions of up to 60 days each.

2.0 WHAT'S MISSING FROM BILL 29

As welcome as many of the proposed amendments are, Bill 29 fails to address some important matters and I recommend that it be amended to do so, as discussed below.

2.1 ENFORCEMENT OF THE LEGISLATION

Bill 29 would amend the powers of the Information and Privacy Commissioner but would not address some key weaknesses in the Act. The proposed amendments would authorize my office to initiate a privacy investigation in the absence of a complaint. Bill 29 would also require public bodies to report to my office on their implementation of recommendations made in a privacy investigation (but not in response to an access to information appeals). These are welcome but do not go far enough, as discussed below.

Meaningful enforcement of rulings—A key shortcoming of Bill 29 is that it would continue to give public bodies the unacceptable ability to ignore adjudicated decisions by the Information and Privacy Commissioner. Some Canadian jurisdictions give their Information and Privacy Commissioners the authority to make decisions, but only to recommend to public bodies that they comply. Several other jurisdictions give their Information and Privacy Commissioners order-making powers. This is the case in Prince Edward Island, Quebec, Ontario, Alberta and British Columbia.[21] Most recently, Newfoundland and Labrador has enacted a stronger form of enforcement, with a direct role for the courts to ensure compliance with decisions of the Information and Privacy Commissioner while providing oversight of those decisions.

By contrast, Northwest Territories public bodies can pick and choose which decisions they will respect and which they will not. From a rule-of-law perspective this is an unacceptably weak regime. It is also not clear why access to information—which the Supreme Court of Canada has stated has constitutional dimensions[22]—does not merit better protection. There is no public policy case for continuing this situation. It is time for the Northwest Territories to ensure that it is not open to public bodies to decide whether or not to respect the law, as adjudicated by the Information and Privacy Commissioner.

Some observers might argue that this is not desirable. They might argue that the recommendations-only approach is preferable as a practical matter, on the basis that it encourages co-operation and facilitates settlement of access to information appeals. They

[21] In all of these cases Information and Privacy Commissioner decisions are subject to judicial review in the courts, which ensures effective oversight by the courts.
[22] *Ontario (Public Safety and Security) v. Criminal Lawyers' Association*, 2010 SCC 23.

might argue that the adversarial model of adjudication negates this advantage. I am aware of no evidence that any such practical advantage is so clear and overwhelming that it warrants leaving the decisions of my office toothless and open to being ignored. It cannot plausibly be argued that the recommendations-only approach is more productive and constructive.

Nor is there any argument in principle against a mechanism to require public bodies to comply with decisions. Many statutory decision-makers who are charged with enforcing important rights—including human rights, employment standards and labour relations matters—are empowered to issue binding decisions. These matters involve both private and public sector organisations. Why is the public sector subject to binding decisions in so many other areas, but not when it comes to access to information? No plausible argument has been made to justify this state of affairs. The public interest in access to information, and the constitutional dimensions of access to information, mean that a proper enforcement mechanism is needed. Any countervailing public interest in the confidentiality of public body information is amply protected under the Act and respected in my office's decisions under the Act where the public body makes its case. It should not be left to public bodies to pick and choose which access to information rights they will respect.

This discussion extends equally to enforcement of the Act's privacy provisions. The Supreme Court of Canada has affirmed on many occasions that privacy has constitutional dimensions. All of the above arguments for an order-making power apply with equal force in relation to the Act's privacy provisions. If the Information and Privacy Commissioner decides, for example, that a public body is collecting citizens' personal information without authority under the Act, there should be a mechanism for requiring the public body to stop violating citizens' privacy. It should not be left to public bodies to pick and choose what privacy rights they will respect.

The best approach, in principle and practice, would be for the Information and Privacy Commissioner to be given order-making powers, as is the case in Prince Edward Island, Quebec, Ontario, Alberta and British Columbia. At the very least, the Act should be amended to adopt the enforcement approach now taken in Newfoundland and Labrador.

Under that province's *Access to Information and Protection of Privacy Act* the Information and Privacy Commissioner adjudicates access to information matters but continues to make recommendations only. However, a public body now has two choices, to comply with the recommendations or to apply to the Supreme Court of Newfoundland and Labrador for a declaration that the public body is not required to comply with the recommendation. Failing such a declaration, the public body must comply with the Information and Privacy Commissioner's decision.

This model could maintain the efficiency and informality of the ombudsperson model while shifting the onus of seeking court review to public bodies, which are far better-placed in terms of having the resources to do so.[23] Keeping in mind that approximately 90% of recommendations are accepted by public bodies,[24] the extra burden on public bodies would not be that significant, particularly if it also results in better submissions to the IPC and thus higher-quality outcomes.

There are areas where I believe my office should have direct order-making power, such as disputes about access to information fees, time extensions and cases in which a public body wishes to ignore an access request that is frivolous or vexatious.[25]

Compelling records for investigations and adjudications—It is also desirable, in light of a recent Supreme Court of Canada decision, to further clarify the powers of the Information and Privacy Commissioner to obtain and view records where necessary for the purposes of reviewing a public body's decision to refuse access.

Section 49.4 of the Act authorizes the Information and Privacy Commissioner to require the production of and examine any record to which the Act applies, despite "any other Act or any privilege available at law".

As discussed below, this language permits my office to require a public body to give us records over which solicitor-client privilege is claimed, so that we can consider whether the alleged privilege is made out. However, my office fully respects the fundamental importance of solicitor-client privilege. For this reason, we rarely compel production of allegedly privileged records and do so only where it is absolutely necessary to do so, where there is no alternative.[26] In the vast majority of the reviews we conduct there is no need to do this. We are, in fact, able in almost all cases to decide the issue based on a description of the nature and purpose of a record (*e.g.*, a description that a record is a legal opinion authored by a named lawyer for the public body). Nonetheless, because there will continue to be rare cases where

[23] Moreover, this onus would be appropriate in principle because it would public bodies, whose decisions are under review in the first place, to the test of standing by the correctness of their decisions and not my office's decisions.

[24] It is not an answer to suggest that, because some 90% of my office's recommendations are respected, change is not needed. The 10% of cases in which the findings and recommendations are ignored almost certainly represent many of the most important cases, where the public interest in compliance is highest. These are, in other words, likely the cases that most require a real enforcement backstop.

[25] 2015 submission, page 46.

[26] This is the standard that courts apply when the decide whether it is necessary for them to view records for which solicitor-client privilege is claimed.

we must view a record to decide a claim of privilege, the power to compel their production remains necessary.

In my view, section 49.4's reference to "any privilege available at law" includes any claim of solicitor-client privilege, meaning legal professional privilege and litigation privilege. However, the Supreme Court of Canada has recently affirmed that a statutory power to compel production of records despite a claim of solicitor-client privilege can be enacted, but it must be clear and unequivocal.[27] That decision, *University of Calgary*, is not binding in relation to section 49.4, including because it dealt with language in AB FIPPA that differs from our provision. In addition, a recent Saskatchewan Court of Appeal decision, which dealt with language identical to section 49.4, has affirmed that this language is sufficiently clear and unequivocal to authorize Saskatchewan's Information and Privacy Commissioner to compel such records.[28]

For greater certainty, however, I recommend that this be made even clearer by adding, immediately after "at law", the words "including legal professional privilege or litigation privilege". I also recommend, for greater certainty, that section 49.4 be amended by adding a new subsection that affirms that production of privileged records to my office, voluntary or compelled, does not waive the privilege. Section 44(2.1) of BC FIPPA contains such language.

In closing, it must be emphasized again that production of allegedly privileged records to my office is only compelled where it is absolutely necessary for my office to view those records in order to determine whether a public body's claim of privilege is made out. It must also be underscored that my office never discloses records whether or not we have determined are privileged or not privileged. Regardless of our finding, only the public body in question actually discloses the records. Further, a court reviews our decisions on privilege using the correctness standard of review, as would doubtless continue to be the case under the above-recommended enforcement model. This means the court owes, and will owe, no deference to our decisions, being able to substitute its own decision on privilege. This fully protects privilege in public body records.

2.2 DUTY TO DOCUMENT DECISIONS & ACTIONS

As I recommended in my 2015 submission, the Act should be amended to include a duty to document key government decisions.[29] This becomes more important each year. As the territory moves further down the road of electronic information systems and the electronic management of government information, a key component should be a duty to adequately,

[27] *Alberta (Information and Privacy Commissioner) v. University of Calgary*, 2016 SCC 53 [*University of Calgary*].
[28] *University of Saskatchewan v. Saskatchewan (Information and Privacy Commissioner)*, 2018 SKCA 34.
[29] 2015 submission, page 50.

appropriately, document government decisions. A proper record of key government decisions and actions is a vital part of good government. It is necessary for the fiscally-sound and efficient administration of publicly-funded programs and services. It underpins the accountability of executive government and key public agencies, including through access to information; it is part of the foundation of a proper archival and historical record.

A number of jurisdictions around the world have recognized this and have created a duty to document. Leading examples are the State of Queensland and British Columbia. In each case, a statutory duty to document decisions and actions is created but detailed guidance is left to the government archivist or similar expert. To be clear, none of the examples assessed for this submission comes close to requiring each and every decision or action to be documented. This would be absurd. What is needed, however, is a core duty to document significant decisions, determined agency-by-agency in accordance with central guidance.

In Queensland, for example, the State Archivist has issued detailed guidance under the *Public Records Act, 2002* that, among other things, requires each state agency to "create complete and reliable records":

> Complete and reliable records provide evidence of activities of the agency and allow the business to operate effectively. Agencies must ensure complete and reliable records are created and retained as appropriate by:
>
> - identifying all the records that allow the business to operate – these provide evidence of decisions, support accountability and transparency, mitigate risk, help the agency meet legislative requirements and reflect the business of the agency
> - specifying how these records must be created, when they must be created, the format they must be created in, who must create them and implementing security and preservation requirements associated with those records
> - integrating record creation into existing business processes
> - ensuring recordkeeping is considered when decisions are made about business systems (particularly decisions around migration and end of life).[30]

As another example, British Columbia's *Information Management Act* will, when amendments passed in 2017 come into force, require provincial government ministries and other core government agencies to document certain decisions.[31] Each such body will be required to

[30] *Records governance policy*, State Archivist, State of Queensland: https://www.qgcio.qld.gov.au/documents/records-governance-policy.

[31] *Information Management (Documenting Government Decisions) Amendment Act, 2017* (Third Reading, March 15, 2017, in force by regulation) [amending Act]: https://www.leg.bc.ca/parliamentary-business/legislation-debates-proceedings/40th-parliament/6th-session/bills/third-reading/gov06-3.

ensure that "an appropriate system is in place within the government body for creating and maintaining, in accordance with applicable directives or guidelines" issued by the provincial government's chief records officer "an adequate record of that government body's decisions".[32]

The necessary amendments could be made to the Act or, perhaps more appropriately, to the *Archives Act*. What is clear, however, is that a statutory duty to document is needed, in the interests of accountability and good government.[33]

2.3 ROUTINE DISCLOSURE OF RECORDS

As noted elsewhere in this submission, access to information is recognized as being of fundamental importance to the accountability and transparency of public institutions. The right of access to information under the Act is therefore a key tool for the public to hold public bodies accountable.

The right for citizens to make individual access requests for specific records is not, however, the only method for making government information available to citizens. As other jurisdictions have recognized, the routine, proactive disclosure of records without access request can be a cost-effective supplement to access requests. The United Kingdom's *Freedom of Information Act 2000* and BC FIPPA, for example, include requirements for proactive, routine disclosure of records. Many provinces, including Ontario and Alberta, also have rules requiring routine disclosure of public servants' remuneration.

Consistent with the recommendation in my 2015 submission, therefore, Bill 29 should be amended to include a framework for the routine disclosure, without request, of certain records.[34] Bill 29 would go part way by introducing a new section 72(1) of the Act. Section 72(1) would require each public body to "establish categories of records … to be made available on demand" without an access request. This proposal would still require someone to make a "demand" for such records.

I would prefer to see a requirement for public bodies to publish certain records proactively, ideally on their websites, and without a "demand". If the demand element is to be retained, public bodies should be required to publish lists of the categories of records that are routinely

[32] Section 5 of the amending Act, which will enact section 19(1.1) of the *Information Management Act*.
[33] Consistent with the discussion below about use of private email and messaging accounts, there is also a need to address, either in the legislation or in regulation, the use of personal devices and accounts (email, text messages, *etc.*) outside of a public body's system, and to ensure that public body decisions that are to be documented are not documented in private accounts.
[34] 2015 submission, pages 2-3.

available on demand. Consideration should also be given to a backstop for this new duty. Specifically, the responsible minister should also be empowered to establish categories of records that are to be disclosed without request, with government departments and cities being required to disclose such records as directed by the minister.[35]

On this point, I believe that routine disclosure should be made of records such as statistical surveys, opinion polls, environmental impact assessments, pollution monitoring data, reports of pollution spills, contract award information. There should also be a duty to disclose the remuneration of each public body employee who earns more than, for example, $100,000.00 in salary or wages each year, together with information about employee benefits.

2.4 OTHER NECESSARY ACCESS TO INFORMATION AMENDMENTS

Coverage of housing corporations—It is extremely important that Bill 29 be amended so that housing authorities under the *Housing Corporation Act* are included within the definition of public body.

As noted in my 2015 submission, my office has received many access requests and privacy complaints about government-funded housing organisations.[36] From a transparency and accountability perspective, it is important to note the importance of these corporations in the lives of their residents, and communities. Further, these organisations spend public money, which is another reason for their coverage to be secured through Bill 29.

From a privacy perspective, housing corporations collect, use and disclose significant amounts of personal information about their residents. This includes financial information, information about their employment and personal information about their family situation. It can also include sensitive information about any conditions that a resident may have. The many privacy complaints my office receives show a clear need for these corporations to live under the same privacy rules as other public sector actors. The Act's privacy-related provisions will not impede their work while also ensuring that the privacy of housing corporation residents is respected.

Restricting use of private email and social media for official business—Another gap in the legislative scheme is the need to ensure that government employees do not attempt to avoid the right of access by using personal email or social media services.

[35] The model for this recommendation is section 71.1 of BC FIPPA.
[36] 2015 submission, page 53.

Although emails created using a private email account are almost certainly going to be within a public body's custody or under the control, and thus subject to the Act, making this clear through appropriate rules is necessary for two reasons. First, clear rules would avoid most uncertainty around coverage of such emails for access to information purposes. Second, such rules would greatly reduce the risk that personal information of citizens is not adequately protected, as will be the case with free, web-based email, which is not encrypted.

These rules could perhaps be put into the Act itself, although the preferred route would be to create a new regulation-making power and then pass the appropriate regulations. A third alternative would be to issue policy-based rules on the matter.[37] Regardless of how this is achieved, the need for rules that apply to *all* public bodies is abundantly clear.

The ideal would be a requirement that all public body business be conducted using work-issued email, with an express prohibition on use of private email, social media accounts or messaging apps for public body business. An exception might be made for exigent circumstances, where work-issued accounts are temporarily not available.[38] In these limited cases, employees should be required to copy their work email on any work-related email they send from a personal account and, where they do not respond, to forward to their work account any emails they receive.

Protecting the identity of access requesters—Although it is convention not to disclose the identity of access requesters within a public body, there is no legal bar to doing so. The Act should be amended to prohibit disclosure of the identity of a requester at any stage before the public body has responded to the request.

2.5 ENHANCING PRIVACY PROTECTIONS

Bill 29 fails in important respects to properly secure the privacy rights of citizens. The vital importance of privacy in our modern society has been affirmed many times. This is especially important as governments seek to collect, use and disclose ever-more information about each of us, information that is often very sensitive. The risks of over-collection and excessive sharing of personal information within government are growing. The privacy risks of increasingly prevalent electronic information systems are clear. The following concerns should be addressed but Bill 29 fails to do this. The Bill should be amended to deal with these concerns.

[37] This would not reach local governments or housing corporations, however, if issued by the territorial government. This would create an undesirable gap.

[38] For example, where a work-issued phone malfunctions or there is a government-wide email system shutdown.

Privacy breach notifications—Bill 29 would not keep pace with legislative developments across Canada in respect of requirements for public bodies and private sector organisations to notify individuals whose personal information has been affected by a privacy breach (*i.e.*, unauthorized access to, or collection, use or disclosure, or loss of their personal information). While it is true that the recent legislative focus has been on private sector privacy laws, with governments being reluctant to require themselves to notify citizens when there has been a privacy breach, public sector breach notification requirements are going to spread. This is the time for the government to ensure that our public bodies notify citizens of breaches that affect their personal information.

The duty to notify individuals of a breach that meets a statutorily-defined risk of harm is necessary for several reasons. First, it enables those affected to protect themselves from identity theft or fraud, and in some cases from personal harm. Second, the duty to notify affected individuals, and the public, serves as an important incentive for governments to take privacy seriously and avoid breaches in the first place. Third, a breach notification requirement would require public bodies to investigate the details of breaches, notably how they happened, and thus give them a solid information base for steps to prevent similar breaches in the future. The requirement to notify would, in other words, present key learning opportunities and contribute to improved privacy practices in the future.

It is therefore time for the territorial government to recognize this and enact a duty for the territorial government and all other public bodies to notify affected individuals of a privacy breach involving their personal information. Such a step in our territory would not be unique. Nunavut, for example, has since 2012 had a comprehensive breach notification process for public bodies[39] and Newfoundland's new legislation contains similar provisions. In addition, Ontario's *Personal Health Information Protection Act* has for some years included a breach notification requirement, as does section 87 of our own *Health Information Act*.

The section 87 duty arises where personal health information about an individual is used or disclosed other than as permitted by the *Health Information Act*, is lost or stolen, or is altered, destroyed or otherwise disposed of without authorization. Notice must be given to the affected individual as soon as reasonably possible. This might be a starting point for a privacy breach notification scheme under the Act.[40] That said, I believe the Nunavut example ought to be given serious consideration as a model for the Northwest Territories.

[39] *Access to Information and Protection of Privacy Act*, sections 49.7 through 49.14

[40] I acknowledge that recent federal legislative changes (through amendments to the federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act*, respecting breach notification) and legislation in Alberta (Alberta's *Personal Information Protection Act*) require notification only where there is a real

Sharing of personal information for common or integrated programs—Bill 29 would add a new definition of "common or integrated program or service", being "a program or service that provides one or more services through a public body working collaboratively with one or more other public body [*sic*], or with an agency or a combination of public bodies and agencies".[41] Sections 41 and 48 would be amended to authorize public bodies to disclose and collect personal information where necessary for the delivery of a common or integrated program or service.

I recognize that governments increasingly are taking a joined-up approach to service delivery. Existing silos between government departments are being broken down, so that citizens can receive collaboratively-delivered expert services. Such integrated services are often seen in the social services sector, where high-needs clients may require expert support and resources found in more than one department. While I recognize the trend, and the need to support collaborative service delivery, the amendments need to be tightened up.

The key issue here is the very broad, ill-defined, scope of what can qualify as a common or integrated service or program. At the very least, it should be necessary for the existence and nature of the supposed service or program to be documented through a form of agreement among the participating public bodies.[42] The agreement would be completed after the PIA has been completed and it would describe the personal information that will be collected, used and disclosed. There should also have to be senior executive approval of the PIA and service agreement before it can begin.

Privacy impact assessments should be mandatory—The Act does not, at present, require public bodies to conduct a privacy impact assessment (PIA) when a program, activity or system

---

risk of "significant" harm, whereas the *Health Information Act* does not require there to be a risk of "harm" from the breach. If a harms test is added to the Act, the risk should not be one of "significant" harm. It is neither fair nor reasonable to shift the burden to citizens of enduring the risk of harm by requiring notification only where the risk is "significant". Why should citizens bear any risk of harm? What incentive would there be for government to properly protect citizens' personal information in lesser cases. Citizens have no choice but to allow government to collect their information in the first place. They vote with their wallets, as they can in their private dealings, by refusing to deal with businesses that have poor privacy track record. This is another argument for a lower public sector threshold.

[41] First, use of the singular as noted above appears to be a typographical error. Second, the term "agency" is not defined in Bill 29 or the Act, or the *Interpretation Act*, so the breadth of its meaning is not clear. It may be intended to cover only agencies prescribed as public bodies by regulation under the Act, but this is not at all clear. This should be clarified.

[42] This is of course also desirable to ensure that the participants are clear as to each other's duties, clear about governance, and clear about who pays for what and how.

involving personal information is being created or amended. It should do so, and Bill 29 should be the vehicle to do that.

PIAs have for many years now been recognized as a basic tool of good privacy practice in government. They help public bodies decide whether an initiative they are considering may be problematic from a privacy-compliance perspective. PIAs help ensure that initiatives proceed only if there are no compliance concerns that cannot be mitigated. They enable what is known as privacy by design, with privacy compliance being designed into the initiative at the outset. PIAs also enable public bodies to assess whether, even if an initiative is legally compliant, it is not good policy from a privacy perspective.

A PIA is an important and highly-desirable business risk assessment tool and should be mandatory. Bill 29 should amend the Act to require territorial departments and cities to complete a PIA for any proposed system, project, program or service, whether new or amended. Consideration should also be given to requiring each PIA to be submitted to my office for comment.[43]

Last, the Act should require that all completed PIAs be made publicly available through the routine disclosure provisions discussed above.

2.6 REMUNERATION OF THE COMMISSIONER

My last concern about Bill 29 is that it would miss the opportunity to address a worrisome aspect of the Act, a matter that should be dealt with—how the remuneration for the next Information and Privacy Commissioner will be set. Looking ahead, past my tenure, the independence and impartiality of future Information and Privacy Commissioners must not continue to be open to question because they have to negotiate their remuneration with the territorial government. Concerns around real or apparent conflict or bias on the part of our independent judiciary and tribunals have caused legislatures to introduce independent mechanisms to set remuneration of judges and tribunal members. This policy concern needs to be addressed in the Act.

The British Columbia approach is to stipulate in BC FIPPA that the remuneration of the Information and Privacy Commissioner is that of the chief judge of the Provincial Court of

[43] I am not proposing that my office would approve PIAs, including because it is necessary to keep my office free to respond later to any complaints related to a PIA's subject-matter.

British Columbia.[44] I am not necessarily recommending the same approach, though a similar provision could be introduced (with the remuneration being pro-rated if the position continues to be part-time). Another approach would be similar to that in Saskatchewan, which provides that the salary of the Information and Privacy Commissioner is "equal to the average salary of all the deputy ministers and acting deputy ministers of the Government calculated as at April 1 in each year".[45] A last option might perhaps be to require a committee of the Legislative Assembly to unanimously set the Information and Privacy Commissioner's remuneration. The overall aim must, again, be to ensure that the impartiality and independence of the Information and Privacy Commissioner cannot be questioned because he or has had to bargain with the government or with the legislative assembly for appropriate remuneration.

3.0 CONCLUSION

As this submission makes clear, Bill 29 would enact some very welcome changes to the Act. it would promote efficiency in some areas and make some desirable substantive changes. I support those aspects of Bill 29. However, for reasons given above, some aspects of Bill 29 are problematic and should be changed or withdrawn. Bill 29 also fails to grapple with some vitally-important issues, such as the need for proper enforcement of my office's decisions. accordingly, while I commend the government for the positive aspects of Bill 29, I strongly believe that changes to it are necessary and urge the government to make those changes before Bill 29 proceeds any further.

***

[44] Section 40, which also states that the Information and Privacy Commissioner is entitled to participate in the public service pension plan.
[45] *Freedom of Information and Protection of Privacy Act*, section 41(1).