

## FIRST READING SPEAKING NOTES

Bill XX – 2021

*Freedom of Information and Protection of Privacy Act, 2021*

---

[After “Introduction of the Bill” is called]

The Minister stands to be recognized by the Speaker.

[The Speaker calls upon the Minister.]

**Mr. Speaker, I have the honour to present a Message from Her Honour the Lieutenant Governor.**

[Chamber staff takes the Message to the Speaker]

The Minister sits

[The Speaker reads the message.]

[The Speaker calls upon the Minister.]

The Minister stands and states:

**I move that the Bill be introduced and read a first time now.**

- **Mr. Speaker, I am pleased to introduce Bill XX. This bill amends the *Freedom of Information and Protection of Privacy Act*.**
- **The Act has not been substantially updated since 2011 and we are quickly falling behind other jurisdictions and advancements in technology.**
- **The COVID-19 pandemic has highlighted people's need for safe and convenient online services.**
- **This bill proposes amendments to ensure government provide the level of service people deserve, keep pace with new technology, and enhance privacy protection.**
- **The changes we're proposing will strengthen government accountability and transparency by enabling us to be more responsive to the needs of people; to add more public bodies; and to charge new offences for destroying records to evade FOI.**
- **By updating FOIPPA's data-residency provisions, we will improve how people access government services, while continuing to ensure that the personal information people trust us with is protected.**
- **By improving B.C.'s high-quality FOI services, we will free up government resources to respond to the thousands of people, businesses and organizations who request access to information every year.**
- **We will also enhance public-sector privacy protections and increase accountability by implementing mandatory privacy breach reporting and increasing penalties for general and privacy offences under the Act.**

- **And we are demonstrating the Province's commitment to diversity, inclusion, reconciliation and equity by increasing information sharing with Indigenous peoples, adding Indigenous cultural protections and removing non-inclusive language.**
- **Indigenous leaders, stakeholders, and public body representatives have been asking for changes for over a decade.**
- **These amendments will address their feedback and make it easier for people to access information, while also maintaining B.C.'s leadership role in safeguarding information.**

The Minister sits

[The Speaker puts the motion.]

[The Speaker calls upon the Minister.]

The Minister stands and states:

**Mr. Speaker, I move that the Bill be placed on the Orders of the Day for Second Reading at the next sitting of the House after today.**

[The Speaker puts the motion.]

## SECOND READING SPEAKING NOTES

**Bill XX – 2021**

***Freedom of Information and Protection of Privacy Act, 2021***

---

[The House Leader calls for Second Reading of Bill XX entitled  
***Freedom of Information and Protection of Privacy Act, 2021***]

The Minister stands to be recognized by the Speaker.

[The Speaker calls upon the Minister.]

### Opening

s.13



s.13

s.13

s.13

s.13

**Closing**

The Minister sits

[Bill is debated]

[When the debate is concluded, the Speaker will recognize the Minister to close debate:]

The Minister stands

The Minister makes final second reading comments followed by:

**And with that, Mr. Speaker, I move second reading.**

The Minister sits

[The Speaker puts the motion]

[The Speaker calls upon the Minister.]

The Minister stands and states:

**Mr. Speaker, I move that the bill be referred to a Committee of the Whole House to be considered at the next sitting of the House after today.**

The Minister sits

[The Speaker puts the motion]

Page 011 of 166 to/à Page 012 of 166

Withheld pursuant to/removed as

s.14

Page 013 of 166 to/à Page 014 of 166

Withheld pursuant to/removed as

s.3



October 20, 2021

Minister Lisa Beare  
Minister of Citizens' Services  
PO Box 9068 Stn Prov Govt  
Victoria BC V8W 9E2

Dear Minister Beare:

**RE: Bill 22 - Freedom of Information and Protection of Privacy Act amendments**

I write regarding the proposed amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA), several of which are of deep concern, while others are very welcome, and I would be happy to discuss my views with you before Third Reading of Bill 22.

Starting with positive aspects of the proposals, I welcome the new requirements relating to privacy impact assessments, the new privacy breach notification rules, and the duty for public bodies to have privacy management programs. The inclusion of snooping offences is also a positive step. These and other constructive changes to FIPPA, discussed below, represent the most extensive amendments since 2011. They will help ensure British Columbia keeps pace with other jurisdictions across Canada and globally.

As discussed below, however, other proposals would be a step backward for British Columbia.

***Absence of information about key regulations***

An overriding concern with Bill 22 is the unknown impact of key amendments because their substance will only be filled in through regulations, *about which we know nothing*. This is of greatest concern in relation to the proposed repeal of the data residency requirements in Part 3 of FIPPA, discussed below. It is crucial for government to disclose now what it intends to do to protect the personal privacy of British Columbians whose personal information may be exported outside Canada.

On this point, I note that it is quite routine for governments to disclose draft regulations for public consultation and legislative scrutiny. For example, the federal government published draft regulations under *Canada's Anti-Spam Law*, giving legislators, regulators, and stakeholders ample opportunity to comment on them. There is no legal or constitutional impediment to doing so here, and I urge you to publish any draft regulations, or details of regulations, for public comment. The issues at stake—particularly respecting the data residency amendments—are too important and meaningful debate depends on everyone knowing what is intended.

At the very least, it is imperative that my office be consulted on the draft regulations, as soon as they are available, as their content will provide the crucial legal substance on data residency protections and other important matters.

### ***Data linking***

I support the proposed improvements to the provisions dealing with data-linking initiatives, which had previously failed to capture many types of data-linking. The new definition of data-linking and related concepts would, in my view, capture the types of programs anticipated in 2011, when the data-linking provisions were enacted.

However, Bill 22 leaves the details of how data-linking activities are to be conducted to regulations, about which we have no details. These regulations must include rules and requirements for data-linking programs that bring transparency to these activities and include protections that are common in other provinces. I urge the government to publish draft regulations at the earliest opportunity, or to provide details of what is intended, and to consult meaningfully with my office about the regulations.

### ***Data residency***

I agree that a new approach to data residency that more closely aligns our privacy laws with other Canadian jurisdictions and the EU's GDPR is necessary. However, as you are aware, I am deeply concerned about how government proposes to do this. The proposed amendments remove the data residency requirement altogether, leaving any protections to regulations, about which we know nothing.

With respect, it is not enough for the government to say that guardrails will be put in place in regulations at a later date. As s. 33.1 currently reads, if the government chooses to not pass a regulation there will be **no** protections at all for personal information disclosed outside of Canada. Further, unlike the development of other regulations, such as those regarding data-linking (s. 76(2.1), government is not required to consult me—or anyone else—on the development on data residency regulations (s. 76.1).

Without real assurances that meaningful protections will be put in place, this proposal represents a step backwards by British Columbia at a time when other jurisdictions are modernizing their data residency requirements, as Quebec did with its recently enacted Bill 64. Again, I am not opposed to a modernization of data residency, but our personal information needs to be protected with appropriate, and known, safeguards.

Among other things, the regulations should require public bodies to conduct privacy impact assessments before deciding whether to export personal information. These assessments should

include considerations such as the sensitivity of personal information, the purpose of the disclosure, the contractual or other measures in place to provide real protections, and the legal framework of the foreign jurisdiction involved. Another possible factor, which seems eminently reasonable and was recommended to the last Special Committee by major stakeholders, was to require public bodies to assess whether there is a reasonable alternative in Canada to a proposed export of personal information.

### ***Proposed privacy breach notification rules***

As noted earlier, I support the introduction of privacy breach notification requirements. These are important protections for British Columbians. I note, however, that proposed s. 36.3(3) would not enable a public body to hold off on notifying affected individuals where disclosure of the breach could compromise a criminal investigation. I believe that such an exception should be added to s. 36.3(3), which would be consistent with similar provisions elsewhere.

### ***Disclosure harmful to interests of an Indigenous people***

I welcome the addition of s. 18.1, which would require public bodies to refuse to disclose information that could affect a range of specific rights and interests of Indigenous peoples. I also welcome the addition of s. 18.1 to s. 23, which would require public bodies to consult Indigenous people about possible disclosure of information in appropriate cases.

### ***Subsidiary corporations***

I was encouraged to see changes enabling the addition of subsidiary corporations and other entities as public bodies. I am concerned, however, that this would be achieved by the Minister, using a discretionary order-making power to add an entity if the Minister concludes it is in the public interest. There are no criteria governing when this should be done. The recent concern about InBC investment corporation not being made subject to FIPPA—as it clearly ought to be—is an example of why this change does not go far enough.<sup>1</sup> At the very least, I call on the government to ensure that it consults with my office about entities that could be covered.

### ***Removal of the Office of the Premier as a public body***

I am very concerned that Bill 22 would remove the Office of the Premier as a public body under Schedule 2 of FIPPA. My understanding is that the government believes this designation is not necessary, on the basis that the Premier, a first minister, is a minister and therefore his office is a ministry, and is therefore covered by the Schedule 1 definition of “public body”.

This is not, with respect, clear in law or constitutional convention, and this change would introduce,

---

<sup>1</sup> For more information see my May 19, 2021 letter on this issue: <https://www.oipc.bc.ca/public-comments/3540>

at the very least, uncertainty in the application of the law. Moreover, I am not aware of any harm flowing from retaining this designation, which obviously begs the question as to why the change is being made when the outcome is, again, not as clear as I am told government believes it is.

The Office of the Premier lies at the heart of provincial governance. I call on the government to delete this proposal from Bill 22, for greater certainty that FIPPA's transparency and accountability provisions will continue to apply, as they have for decades, to the Office of the Premier.

### ***Addition of a new public body***

By contrast, I support the amendment to designate the BC Association of Chiefs of Police and the BC Association of Municipal Chiefs of Police as public bodies under Schedule 2 of the Act. This is a longstanding recommendation from my office and is a welcome enhancement.

### ***Fines for destruction of records***

The Bill will make it an offence for a person to wilfully conceal, destroy or alter any record to avoid complying with a request for access. This is a step in the right direction, but it does not go far enough. The inappropriate destruction of records should be penalized anytime, not only when there is an access to records request in play. This should include oversight over destruction of records other than in accordance with approved disposal schedules, as is the case under Alberta's *Freedom of Information and Protection of Privacy Act*

### ***Snooping offences***

I welcome the creation, in a new s. 65.4, of several privacy-related offences, offences intended to deter the unauthorized collection, use or disclosure of personal information. Such offences—commonly known as “snooping offences”—do occur and must be deterred and punished appropriately. I am concerned, however, that the offences would not include the “viewing of”, or mere “access to”, personal information. The government may believe that this kind of intrusion is covered by the offence of collecting personal information, but I am concerned that this is not as clear as it should be, i.e., it is not entirely free from doubt that an individual's mere observation of personal information is a collection of that information.

On this point, Bill 22 would remove from s. 30 the duty of public bodies to implement reasonable security measures to guard against unauthorized “access” to personal information, perhaps for the reasons just outlined, and this is also of concern. I ask that this change to s. 30 not be made, and that s. 65.4 create the offence of “accessing” personal information contrary to Part 3.

### ***New exclusions of records from FIPPA***

Another significant concern is that the right of access under FIPPA would no longer apply to certain

electronic records, a change that would in turn limit public bodies' duty to create records from electronic records.

A new s. 3(3) would provide that Part 2 of the Act—FIPPA's access to information provisions—no longer applies to either of the following records:

- a record that does not relate to the business of the public body;
- a record of metadata that
  - (i) is generated by an electronic system, and
  - (ii) describes an individual's interaction with the electronic system;
- an electronic record that has been lawfully deleted by an employee of a public body and can no longer be accessed by the employee.

The first of these exclusions from Part 2 is of concern because it is both potentially very broad and ambiguous. While this might not exclude all third-party information from Part 2, I am concerned that this provision will be used to reject access requests where they touch on a record that contains third-party information. Setting aside the issue of what the phrase “relate to” means, I am concerned that the concept of the “business of” a public body” is both over broad and unclear, and how it is far from clear how that would be determined case by case. With respect, no persuasive case can be made for this exclusion for the public's right of access, which would be out of step with Canadian access to information laws.

I am also deeply concerned that excluding a record of metadata will hinder the interests of transparency and accountability. Metadata associated with a record can, for example, enable useful analysis of how particular records have evolved over time. This can significantly enhance public understanding of who is responsible for a record, and for its evolution. The proposed exclusion of such information from the right of access is worrisome.

### ***Application fees for access requests***

Bill 22 would authorize the government to impose application fees for access to information requests, fees that could be charged by all types of public bodies. This would be a significant step in the wrong direction. Application fees pose a real barrier for many who seek information that should be readily available to the public. I am unable to understand how this amendment improves accountability and transparency when it comes to public bodies that operate in a free and democratic society. Nor is it necessary, since FIPPA already authorizes public bodies to charge access fees, to help defray the costs of responding to requests.

We are living in a time when people are seeking more answers, and greater accountability, from public bodies and their governments, amplifying the significant role that freedom of information plays in allowing people to get information about what their governments are doing, and the decisions that affect them. To add another barrier of access at a time when transparency is deeply troubling.

Further, I am troubled that there would be no ability for my office to waive an application fee if it is in the public interest.

### ***Authorizing public bodies to disregard access requests***

The amendments expand the grounds on which public bodies can ask my office for permission to disregard access to information requests. Limiting or blocking a right provided by a statute is a serious matter, but there are occasions when it is necessary, as many of this office's decisions under s. 43 affirm.

Each year, my office receives approximately ten such requests and approximately half of those are partially or fully granted. The Bill proposes a troubling new criterion under which I could be asked to authorize a public body to disregard a request where responding to the request would unreasonably interfere with the operations of the public body because the request is "excessively broad." This criterion is only found in one other province.

The narrowing of a request can already be done through consultation with the applicant or through a fee estimate, and I believe that adding this new ground unnecessarily encroaches on the public's right of access.

### ***Error in s. 36 of Bill 22***

Section 36 of Bill 22 proposes a change to s. 61(2) of the Act to add "audit" and remove "review" for consistency. However, in this instance the powers and protections relate to an external adjudicator designated under s. 60 which do not include to conduct an audit. This may unintentionally remove protections for an external adjudicator making a determination under s. 60(b). Therefore, the term "review" should not be removed.

Finally, I believe there are a number of missed opportunities that deserve mention.

### ***Restoring the s. 13 protection for "advice or recommendations" to its original intent***

The exception to access provided for in s. 13(1) of the Act has been eroded by successive, overly broad, judicial interpretations. Despite the clear intention of the Legislature, in s.13(2)(a), that the protection for "advice or recommendations" does not extend to "factual material" underpinning policy advice or recommendations, the courts have effectively curtailed the public's right to access "factual information"—how this differs from "factual material" is not at all evident—that formed the basis for advice or recommendations.

For years, there have been repeated calls for reform by Special Committees of the Legislative Assembly to review FIPPA, by my office, and by many others, to return s. 13(1) to its original intent.

Doing so would in no way impair the ability of public servants to continue to formulate frank advice or recommendations in confidence, which is what the Legislature intended to enable, and no more. It is well past time to make this change and I call on the government to do so in Bill 22.

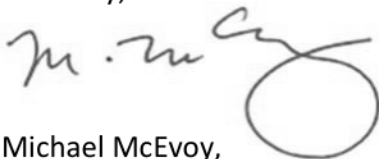
***Special Committee to Review the Freedom of Information and Protection of Privacy Act***

As just suggested, FIPPA provides for periodic review of the statute by an all-party Special Committee of the Legislative Assembly. Several of these have been concluded and many, many useful and important recommendations have been made by these Special Committees, the latest of which has been appointed. It is not at all clear why government has chosen to move forward with amendments ahead of the Special Committee's legislated work to review the Act. The work of the Special Committee is essential, as it is able to pull information and consultations from a variety of sources, encouraging fulsome public dialogue about proposed amendments. I have to question how meaningful the first substantive amendments to the Act in over a decade can be when there is no time for all stakeholders to provide dialogue. To move forward with these amendments, in a year that the Special Committee is tasked to do this work, is baffling.

As I conclude, I believe it is important to reinforce that the purpose of my office, which guides the work we do, is to protect and advance the access and privacy rights of British Columbians, and to serve the public and the public interest. I have reviewed this proposed Bill through that lens.

In the spirit of transparency, and because this letter relates to a Bill now before the Legislative Assembly, this letter will be made publicly available, consistent with my office's longstanding practice.

Sincerely,



Michael McEvoy,  
Information and Privacy Commissioner  
for British Columbia

pc: Honourable Bruce Banman, MLA  
Opposition Critic for Citizens' Services

Honourable Sonia Furstenau, MLA  
Leader of the Third Party

# OUR LAND IS OUR FUTURE

UNION OF BRITISH COLUMBIA INDIAN CHIEFS

FOUNDING HEAD OFFICE  
209 - 345 Chief Alex Thomas Way  
Kamloops, B.C. V2H 1H1  
Tel: 250-828-9746  
Fax: 250-828-0319



VANCOUVER OFFICE  
401 - 312 Main Street  
Vancouver, B.C. V6A 2T2  
Tel: 604-684-0231  
Fax: 604-684-5726  
1-800-793-9701  
Email: [ubcic@ubcic.bc.ca](mailto:ubcic@ubcic.bc.ca)  
Web: [www.ubcic.bc.ca](http://www.ubcic.bc.ca)

November 23, 2021

The Honourable John Horgan  
Premier of British Columbia  
Via email only: [premier@gov.bc.ca](mailto:premier@gov.bc.ca)

The Honourable Lisa Beare  
Minister of Citizens' Services  
Via email only: [CITZ.Minister@gov.bc.ca](mailto:CITZ.Minister@gov.bc.ca)

**OPEN LETTER: Call for the Immediate Withdrawal of Bill 22, *Freedom of Information and Protection of Privacy Amendment Act, 2021***

Dear Premier Horgan and Minister Beare,

On October 18, 2021, your government introduced amendments to British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA) through Bill 22. We have learned that Bill 22 is quickly proceeding through the legislature and is anticipated to receive Royal Assent before the end of the current legislative session on November 25<sup>th</sup>. However, the bill in its current form fails to uphold First Nations' unique rights of access to information as many of the proposed amendments will create new barriers for First Nations requiring access to provincial government records to substantiate their historical grievances against the Crown. Further, several proposed amendments disregard significant concerns we identified in formal submissions to the public engagement process, and introduce measures about which we were never informed, contravening Article 19 of the *United Nations Declaration on the Rights of Indigenous Peoples* (UN Declaration), and your government's legal obligations under the *Declaration on the Rights of Indigenous Peoples Act* (DRIPA).

We call on your government now to withdraw Bill 22 and establish a process of substantive engagement with Indigenous governing bodies affected by the FIPPA to ensure that transparency, openness, and fairness are enhanced and First Nations' rights under the UN Declaration are upheld.

The right to access information is a fundamental component of First Nations' efforts to resolve historical land-related grievances, such as specific claims. Because First Nations are required to produce a wide range of records to substantiate their land claims and historical land-related grievances against the Crown, Freedom of Information has direct impacts on the ability of First



Nations to achieve justice through government mechanisms of redress, a right articulated in Article 28 of the UN Declaration.

In April 2018, the Union of BC Indian Chiefs made a formal submission to the Ministry of Citizens' Services' engagement process in which we identified key barriers First Nations routinely experience when attempting to obtain provincial government records through Freedom of Information, including prohibitive fees and the denial of requests for fee waivers, prolonged delays, overly broad applications of exceptions to disclosure, widespread failures to create, retain, and transfer records, and the exclusion of subsidiaries from duties of disclosure. We emphasized that the barriers faced by First Nations seeking information access must be specifically and systematically targeted, such that rights to redress are advanced and protected.

The provisions in Bill 22 ignore our concerns and further entrench barriers to access. The introduction of an application fee for all Freedom of Information requests will disproportionately harm First Nations requesters since they experience higher levels of poverty and often lack resource capacity. Your characterization of the new fee as "modest" displays astounding ignorance and insensitivity since legal processes of redress for historical losses require First Nations to make multiple formal requests for records from various public bodies in order to obtain evidence. It is nonsensical that a government publicly committed to reconciliation, transparency, and accountability would impose further financial hardships on First Nations who require access to provincial government records to substantiate claims of government wrongdoing. The bill also prevents the Information and Privacy Commissioner from waiving the application fee if the request is in the public interest.

It is especially egregious that the introduction of an application fee was never discussed with First Nations or their representative organizations, and as such contravenes Article 19 of the UN Declaration which requires governments to consult and cooperate in good faith with Indigenous peoples to obtain their free, prior and informed consent before adopting and implementing legislative or administrative measures that may affect them. The provincial government's selective application of Article 19 violates the DRIPA and betrays a colonial attitude toward its implementation.

Bill 22 introduces no penalties for public bodies who exceed legislated timelines for providing requested information, which will do nothing to address delays and the under-resourcing of the information management system which accounts for it. The bill continues to exclude subsidiaries from mandatory disclosure, compromising First Nations' abilities to obtain complete historical records required for their claims to succeed.

Alarmingly, the bill removes the Office of the Premier and Executive Council Operations from the list of public bodies covered by the FIPPA, and fails to create, enforce, or oversee a 'duty to document'. This amounts to willful obstruction and hampers First Nations seeking access to information. While specific claims are historical grievances that occurred at least fifteen years prior to the filing of a claim, this bill effectively absolves your office of any legal responsibility to disclose records related to the actions or decisions which may be subject to future claims. The same can be said about the bill's failure to make it mandatory for public bodies to create records of all actions and decisions, something the provincial NDP championed when it was in

opposition and about which it now, holding a majority in the legislature, seems to regard with disdain.

Advocates for government accountability and transparency, organizations committed to human rights, and the provincial Information and Privacy Commissioner are condemning this bill, calling it a highly unethical step backward. The amendments introduced through Bill 22 as discussed above will have concrete, negative impacts on First Nations' access to justice. This is a fundamental concern for the communities we represent.

We reiterate our call for you to withdraw Bill 22 and take immediate steps to make meaningful, direct dialogue with First Nations a priority. This work must be guided by transparency, due process, and full enactment of the government-to-government approaches articulated within the UN Declaration and outlined in DRIPA.

**On behalf of the UNION OF BC INDIAN CHIEFS**



Grand Chief Stewart Phillip  
President



Chief Don Tom  
Vice-President



Kukpi7 Judy Wilson  
Secretary-Treasurer

CC: UBCIC Chiefs Council  
BC Assembly of First Nations  
First Nations Summit  
Special Committee to Review the Freedom of Information and Protection of Privacy Act

Page 025 of 166 to/à Page 026 of 166

Withheld pursuant to/removed as

s.3

## Biggs, Jackie CITZ:EX

---

**From:** Jason Woywada <jason@fipa.bc.ca>  
**Sent:** October 26, 2021 3:20 PM  
**To:** OfficeofthePremier, Office PREM:EX; Minister, CITZ CITZ:EX  
**Cc:** Mike Larsen; BCLiberalCaucus@leg.bc.ca; greencaucus@leg.bc.ca  
**Subject:** 116075 - Bill 22 amendments to the Freedom of Information and Protection of Privacy Act (FIPPA).  
**Attachments:** 20211026 Bill 22 Coalition Letter to Premier and Minister.pdf

**Follow Up Flag:** Follow up  
**Flag Status:** Completed

**Categories:** Minister Response

**[EXTERNAL] This email came from an external source. Only open attachments or links that you are expecting from a known sender.**

Please find the following correspondence attached and below.

We, the undersigned, believe **transparency matters** and, because of this, we write to you to express our grave concerns about the Bill 22 amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA).

Bill 22 would see substantive changes made to FIPPA for the first time in over a decade. Unfortunately, if passed, this Bill will undermine access to information and make public bodies less transparent. It is a step backwards for openness and accountability, and a missed opportunity to protect the privacy and improve the information rights of British Columbians.

This legislation would extend the ability of current and future governments to keep people in the dark about vital matters of public interest. Its introduction at this time short-circuits the work of the special legislative committee responsible for reviewing FIPPA, preventing meaningful public consultation. If passed, it would immediately put up more barriers for people seeking access to information.

You have made prior commitments regarding the value you place on transparency and about the need to improve government accountability, but this legislation would make it harder for everyone - concerned citizens, experienced researchers, and you - to get facts rather than spin.

We recognize this majority government can readily pass this regressive Bill quickly. If that happens, it will impact the citizens of British Columbia now, haunt us into the future, and set a dangerous precedent across Canada.

Our message is simple: **Transparency matters to all of us. Stop Bill 22.**

We call on the government to:

- Withdraw this Bill
- Recognize the role of the all-party special committee and allow it to complete its work, including an open consultation process
- Commit, on record, to introduce comprehensive amendments to FIPPA that reflect the recommendations of past and current special committees

As interested individuals and members of organizations, we call on you to demonstrate your commitment to democratic values by taking action to im-prove—not reduce—the transparency of public bodies.

Signed by:

BC Freedom of Information and Privacy Association

With support from our partners as attached.

Cheers

Jason Woywada (he/him/his)

Executive Director, BC Freedom of Information and Privacy Association



PO Box 8308 Victoria Main, Victoria BC V8W 3R9

Phone: 604-739-9788

Website: <https://fipa.bc.ca>

Twitter: [@bcfipa](https://twitter.com/bcfipa)

I respect and acknowledge I am working and residing in the unceded Coast Salish Territory of the Lekwungen amongst the Songhees, Esquimalt and WSÁNEĆ peoples whose historic relationships with the land continue to this day.



Your Data  
Your Rights



By email: [Premier@gov.bc.ca](mailto:Premier@gov.bc.ca), [CITZ.Minister@gov.bc.ca](mailto:CITZ.Minister@gov.bc.ca)

October 26, 2021

The Honourable John Horgan M.L.A.  
Premier of British Columbia  
PO Box 9041 Stn Prov Govt  
PROV GOVT VICTORIA, BC V8W 9E1

The Honourable Lisa Beare M.L.A.  
Minister of Citizens' Services  
PO Box 9068 Stn Prov Govt  
Victoria BC V8W 9E2

Dear Premier and Minister,

**Subject: Bill 22 amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA).**

We, the undersigned, believe **transparency matters** and, because of this, we write to you to express our grave concerns about the Bill 22 amendments to the *Freedom of Information and Protection of Privacy Act* (FIPPA).

Bill 22 would see substantive changes made to FIPPA for the first time in over a decade. Unfortunately, if passed, this Bill will undermine access to information and make public bodies less transparent. It is a step backwards for openness and accountability, and a missed opportunity to protect the privacy and improve the information rights of British Columbians.

This legislation would extend the ability of current and future governments to keep people in the dark about vital matters of public interest. Its introduction at this time short-circuits the work of the special legislative committee responsible for reviewing FIPPA, preventing meaningful public consultation. If passed, it would immediately put up more barriers for people seeking access to information.

You have made prior commitments regarding the value you place on transparency and about the need to improve government accountability, but this legislation would make it harder for everyone - concerned citizens, experienced researchers, and you - to get facts rather than spin.

We recognize this majority government can readily pass this regressive Bill quickly. If that happens, it will impact the citizens of British Columbia now, haunt us into the future, and set a dangerous precedent across Canada.

Our message is simple: **Transparency matters to all of us. Stop Bill 22.**

We call on the government to:

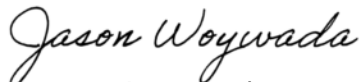
- Withdraw this Bill
- Recognize the role of the all-party special committee and allow it to complete its work, including an open consultation process
- Commit, on record, to introduce comprehensive amendments to FIPPA that reflect the recommendations of past and current special committees

As interested individuals and members of organizations, we call on you to demonstrate your commitment to democratic values by taking action to improve-not reduce-the transparency of public bodies.

Signed by:



Mike Larsen  
President



Jason Woywada  
Executive Director

BC Freedom of Information and Privacy Association  
With support from our partners as attached.

CC:

[BCLiberalCaucus@leg.bc.ca](mailto:BCLiberalCaucus@leg.bc.ca)  
[greencaucus@leg.bc.ca](mailto:greencaucus@leg.bc.ca)

An online version of this letter is [here](#) and is continuing to gain support.

This call to action is supported by the following organizations:

- [The British Columbia Civil Liberties Association \(BCCLA\)](#)
- [The British Columbia General Employees' Union \(BCGEU\)](#)
- [The Canadian Association of Journalists](#)
- [Canadian Centre for Policy Alternatives BC Office \(CCPA-BC\)](#)
- [Canadian Institute for Information and Privacy Studies \(CIIPS\)](#)
- [Centre for Access to Information and Justice \(CAIJ\)](#)
- [The Centre for Law and Democracy \(CLD\)](#)
- [Democracy Watch](#)
- [Fairley Strategies](#)
- [Forest Protection Allies FORPA](#)
- [Independent Contractors and Businesses Association](#)
- [Lawyers Rights Watch Canada](#)
- [Open Media](#)
- [Privacy & Access Council of Canada \(PACC - CCAP\)](#)
- [Public Interest Advocacy Centre \(PIAC\)](#)
- [Student Press Freedom Act Campaign \(SPFA Campaign\)](#)
- [The Union of British Columbia Indian Chiefs \(UBCIC\)](#)
- [West Coast Legal Education and Action Fund \(West Coast LEAF\)](#)
- [The Wilderness Committee](#)



This call to action is supported by the following individuals:

- Jason Austin
- John Brady
- Lynn Copeland
- Carla Graebner, Librarian for Research Data Services and Government Information, W.A.C. Bennett Library, Simon Fraser University
- Sean Holman, Wayne Crookes Professor in Environmental and Climate Journalism, University of Victoria
- Patrick Jardine
- Victoria Lemieux, Associate Professor, Archival Science, School of Information, Co-Lead, Blockchain@UBC research cluster, Distinguished Scholar, Sauder School of Business, Faculty Associate, Institute for Computing, Information and Cognitive Systems, The University of British Columbia
- Lisa P. Nathan, Associate Professor, School of Information, University of British Columbia
- Marcus Ooms
- Dawe Pope
- Ken Rubin, Investigative researcher and transparency advocate
- Dan Schubart
- Chad Skelton, Chair, Department of Journalism and Communication Studies, Kwantlen Polytechnic University
- Stanley Tromp, FOI journalist, researcher
- Maureen Webb, FOI Author

## Biggs, Jackie CITZ:EX

---

**From:** Cook, Jeannette CITZ:EX  
**Sent:** October 28, 2021 11:01 AM  
**To:** Jarmson, Lindsay CITZ:EX  
**Subject:** FW: Best case against the \$25 FOI fee - the citizen applicants

---

**From:** Stromp <stromp@telus.net>  
**Sent:** October 20, 2021 1:42 AM  
**To:** Beare.MLA, Lisa LASS:EX <Lisa.Beare.MLA@leg.bc.ca>  
**Cc:** GCIO Chief Information Officer CITZ:EX <LCTZ.ChiefInformationOfficer@gov.bc.ca>; stromp <stromp@telus.net>; Thomas, Krista CITZ:EX <Krista.Thomas@gov.bc.ca>; Shauna.Brouer@gov.bc.ca; Cook, Jeannette CITZ:EX <Jeannette.Cook@gov.bc.ca>  
**Subject:** Best case against the \$25 FOI fee - the citizen applicants

**[EXTERNAL] This email came from an external source. Only open attachments or links that you are expecting from a known sender.**

Dear Minister Beare, and Chief Information Officer:

Beyond the FOI usage by opposition parties or the (non-Mackin) investigative news media, we need to instead focus on poor, average folk, who can least afford \$25 fees, and would be most harmed, the innocents caught in the political crossfire, the “collateral damage.”

The government assures us that no application fees will be charged for personal requests, just non-personal “general” ones; one problem we have is that the NDP implies that “normal, average” folk usually do not file general requests, and so wouldn’t be harmed by fees. This assumption is mistaken.

Note what B.C. Commissioner McEvoy said in the Sun on the fee – “It poses an obstacle to access and accountability, and not just for media,” he said. “It could be a parent group, for example, that finds itself making access to information requests to multiple health authorities and to the Ministry of Health and other ministries. You could see how that number could add up awfully quickly and be a deterrent to people making legitimate requests.”

David Cuillier, PhD, president, U.S. National Freedom of Information Coalition - “Clearly, \$25 puts many citizens at a disadvantage in interacting with their government – and even worst, it differentially hurts the poor, widening the information gap in our society.... “The public records request system is a way for citizens to interact with their government, and simply should be considered a cost of doing business. So why start making it harder for citizens to know what their government is up to on this front?”

Best of all, my Excel database of 2,000 BC news stories produced by FOI requests can help.  
<https://canadafoi.ca/british-columbia-foi/> I created a new category, not of subject matter, but of a key, overlooked *applicant type* - the average citizen. I wrote:

“For many readers, the most interesting and moving summaries may be found in Category 6 – Personal Requests. These 70 stories are based on FOI requests that were filed not by journalists but by individuals or their family members often in some form of distress. Working to improve their lives, they obtained documents that helped some to clear their names of false allegations, or aided adoptees to find their true parents, or enabled others to obtain redress for childhood abuse, or workplace injuries, botched surgeries, hepatitis C infections, schoolyard bullying, land appropriations and rental evictions. It shows that obtaining records is not solely within the purview of experts, and their usage best demonstrates the professed goal of the FOI law – to empower the average citizen.”

Some of those were from personal requests (with no planned fees), but some also from “general” FOI ones. Importantly, some of these citizens made general requests for their whole community’s benefit, as local activists (many too poor to pay \$25 fees), beyond their own personal interests. And anyways, their personal cases at times reveal a hidden problem shared by hundreds/thousands of others too. See samples below.

-Sincerely yours, Stanley Tromp. [www.canadafoi.ca](http://www.canadafoi.ca)

---

SAMPLES – Fine usage of “general information” BC FOI requests by average citizens, aiding a larger community purpose.

Copyright

Page 035 of 166 to/à Page 041 of 166

Withheld pursuant to/removed as

Copyright

Page 042 of 166 to/à Page 052 of 166

Withheld pursuant to/removed as

s.13

## Biggs, Jackie CITZ:EX

---

**From:** Minister, CITZ CITZ:EX  
**Sent:** August 26, 2021 11:43 AM  
**To:** s.22  
**Cc:** Chouhan.MLA, Raj LASS:EX  
**Subject:** Letter from Minister Lisa Beare

Dear s.22 :

Thank you for your email of July 16. My colleague, MLA Raj Chouhan, asked me to respond on his behalf as the Minister responsible for the *Freedom of Information and Protection of Privacy Act* (FOIPPA), which contains the data residency provisions. FOIPPA is a very important piece of legislation that keeps government accountable to the public and protects the privacy of British Columbians.

As you mentioned, FOIPPA requires information to be stored and accessed only from within Canada, unless an exception applies. COVID-19 has challenged normal business and communication practices, especially in the health sector and for organizations involved in or affected by the public-health emergency. The pandemic has also shown us there is high demand from people for safe and convenient online services. A ministerial order permitting the use of additional communication tools in the public sector during the COVID-19 pandemic is currently in effect until December 31, 2021.

Our government is committed to improving the services businesses, people and families depend on, which requires us to keep pace with their changing needs. We have recently undertaken considerable engagement with Indigenous leaders and various stakeholders, including public sector representatives and members of the public, to better understand what we can do to make government more accountable to people while also safeguarding their personal information. Feedback received will inform our next steps as we look for opportunities to improve government services, increase public accountability and enhance privacy protection.

Thank you for taking the time to send us your thoughts on the data residency issue; it is important to us to hear from stakeholders such as yourself as we consider options going forward.

Sincerely,

Lisa Beare  
Minister of Citizens' Services



Ministry of  
Citizens' Services

**SPEAKING NOTES**  
for  
**MINISTER LISA BEARE**

**BRIEFING FOR CAUCUS**

***FOIPPA AMENDMENTS***

**Date: October 6, 2021**

**Time: 1:00 – 1:30 pm**

**Run Time: Approx. 3 minutes**

## **FOIPPA Amendments Overview**

- **In June, I briefed you on proposed amendments to ensure government can provide the level of service people expect, keep pace with new technology, and enhance privacy protection.**
- **I expect to present the Bill in the house the week of October 18th.**
- **Some of these changes respond to a number of longstanding recommendations from two Special Committees of the Legislative Assembly, the Office of the Information and Privacy Commissioner, the public and other stakeholders.**
- **Highlights of the proposed amendments include:**
  - **Updating FOIPPA's data-residency provisions to allow public bodies to use more modern tools while continuing to ensure that the personal information people trust us with is protected.**
  - **Introducing an application fee for all non-personal FOI requests to address the large and sometimes vexatious requests government receives. This will free up government resources to respond to the thousands of people, businesses and organizations who request access to information.**
  - **Enhancing public-sector privacy protections and increasing accountability by implementing mandatory privacy breach reporting and increasing penalties for offences under the Act.**



- **And we are demonstrating the Province's commitment to diversity, inclusion, reconciliation, and equity by increasing information sharing with Indigenous peoples, adding Indigenous cultural protections and replacing non-inclusive language.**
- **An MLA kit will be coming to your offices shortly before the legislation is introduced to support conversations in the coming weeks on this topic.**

### **Closing Remarks**

- **This act hasn't been updated in nearly a decade and while some stakeholders may make noises about these amendments, many will be very supportive.**
- **We need to make these changes to balance the service we want to deliver with our leadership role in safeguarding information.**
- **Thank you and if there is any additional information you need from my Ministry, or any materials we can provide to you, please don't hesitate to reach out.**

Page 057 of 166 to/à Page 059 of 166

Withheld pursuant to/removed as

s.12 ; s.13

Page 060 of 166 to/à Page 062 of 166

Withheld pursuant to/removed as

s.3

## DECISION NOTE

### Advice to Minister Beare

**Date:** October 5, 2021

**CLIFF#: 116166**

**ISSUE:** Privacy Impact Assessment Directions for Ministry and Non-Ministry Public Bodies

#### BACKGROUND:

Proposed amendments to the *Freedom of Information and Protection of Privacy Act* (FOIPPA) include new requirements related to privacy impact assessments (PIAs), including for ministry and non-ministry public bodies to conduct a privacy impact assessment and to do so in accordance with the directions of the minister (PIA directions). While conducting PIAs in accordance with the PIA directions is the current process for ministries, the amendments will clarify this requirement for non-ministry public bodies.

The purpose of PIA directions is to clarify the legislative requirements for PIAs and to assist public bodies in conducting and documenting PIAs. This includes determining when to complete a PIA and whether the initiative meets the requirements under Part 3 (Protection of Privacy) of FOIPPA. The PIA directions set further requirements for PIAs, which then enable the Corporate Information and Records Management Office (CIRMO) to fulfill its legislated role of reviewing and commenting on ministry PIAs to ensure compliance with FOIPPA.

The PIA directions were last updated in 2014. Updates are required in order to align section references with the amended FOIPPA. Updated PIA directions will also enable a future-state digital PIA process as contemplated following CIRMO's PIA Service Design project in 2019. Further, provisions respecting storage and access of personal information outside of Canada (i.e., data residency) are proposed to be repealed from FOIPPA. s.13

s.13

#### DISCUSSION:

s.13

The PIA directions for non-ministry public bodies are similar to those for ministries; however, they include increased flexibility to reflect the different size and scale of operations for non-ministry public bodies. For example, the ministry PIA directions reflect the central PIA review process in BC government, whereas broader public sector may have diverse internal approaches and processes to achieve compliance, including privacy programs at various stages of development. New PIA directions will assist non-ministry public bodies in conducting PIAs in alignment with their legislative requirements while preserving as much process flexibility as possible.

**OPTIONS:**

s.13

**RECOMMENDATION:**

s.13

*(please circle)***APPROVED****NOT APPROVED****OPTION** \_\_\_\_\_

---

**Lisa Beare**  
**Minister**

---

**Date**

Contact: Kerry Pridmore, 778-698-1591



## PRIVACY IMPACT ASSESSMENT DIRECTIONS

**TO:** HEADS OF ALL MINISTRIES

**DIRECTION:**



**SUBJECT:** Directions to heads of ministries on conducting privacy impact assessments

**AUTHORITY:** These directions are issued under section 69 (5) of the *Freedom of Information and Protection of Privacy Act*.

**APPLICATION:** These directions apply to heads of all ministries.

**EFFECTIVE DATE:** Month Day, Year

---

Honourable Lisa Beare  
Minister of Citizens' Services

## **Minister of Citizens' Services**

### **Directions to Heads of Ministries issued under Section 69 (5) of the *Freedom of Information and Protection of Privacy Act***

I, Lisa Beare, Minister of Citizens' Services (the Minister), issue the following directions to heads of ministries under section 69 (5) of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 (the Act).

These directions repeal and replace Direction 1/14 issued May 9, 2014.

#### **A. Preamble**

##### **Relevant Legislative Requirements**

Section 69 (5) of the Act requires the head of a ministry to conduct a privacy impact assessment (PIA) and must do so in accordance with the directions of the Minister responsible for the Act.

Additionally, when an initiative is a proposed initiative (as opposed to an existing one) section 69 (5.1) of the Act requires the head of a ministry to submit a PIA for the Minister's review and comment. The Act further requires that the PIA for a proposed initiative be submitted during the development phase of the initiative.

##### **Purpose**

The purpose of these directions is to:

1. Direct ministries in determining when a PIA must or may be conducted.
2. Direct ministries in conducting and documenting a PIA that will:
  - a. Determine whether their initiative meets or will meet the requirements under Part 3 of the Act; and
  - b. Identify and assess privacy risks and identify a risk response(s) that is proportionate to the level of the risk.

## **B. Definitions**

In these directions:

“common or integrated program or activity” has the same meaning as in the Act;

“data-linking program” has the same meaning as in the Act;

“head” has the same meaning as the head of a public body that is a ministry in Schedule 1 of the Act;

“initiative” means an enactment, system, project, program or activity;

“ministry” means a ministry of the government of British Columbia;

“personal information” has the same meaning as in the Act;

“personal information bank” has the same meaning as in the Act;

“personal information directory” means the public registry required by section 69 (2) of the Act, which contains summaries of British Columbia government holdings with respect to personal information banks, health information banks, information sharing agreements, and privacy impact assessments;

“privacy impact assessment” (PIA) has the same meaning as in the Act;

“privacy risk” includes:

- an inherent risk of unauthorized collection, use, disclosure, or storage of personal information; and
- something that may inappropriately override or otherwise limit personal privacy.

The level of risk may vary based on:

- the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information; and
- the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information.

“service provider” has the same meaning as in the Act.



## **C. When a PIA must or may be conducted**

1. The head of a ministry must conduct a PIA:
  - a. on a proposed initiative when no PIA has previously been conducted. A previously conducted PIA includes a PIA conducted in consultation with the Minister responsible for the Act, on behalf of all or multiple ministries; or,
  - b. s.13
2. The Minister responsible for the Act may recommend that the head of a ministry conduct a PIA subsequent to an investigation under the Information Incident Management Policy.
3. Where a head of a ministry is not required to conduct a PIA by items 1-2, above, they may conduct a PIA at their discretion and in accordance with these directions.

## **D. General directions on conducting a PIA for an initiative that is not an enactment**

When conducting a PIA for an initiative that is not an enactment, the head of a ministry must do the following:

1. Identify the purpose or objective of the initiative.
2. Identify the information elements, including personal information, to be collected, used, disclosed, or stored, and confirm that the personal information elements are necessary for the purpose of the initiative.
3. Where applicable identify:
  - a. how and from whom the personal information will be collected;
  - b. how the personal information will be used;
  - c. how and to whom personal information will be disclosed; and,
  - d. if an assessment of disclosure for storage of personal information outside of Canada is required, as per E.
4. Identify relevant legal authority (or authorities) authorizing the collection, use, or disclosure of personal information, as applicable.
5. If the initiative involves personal information, identify privacy risks and privacy risk responses that are proportionate to the identified risks.

6. Identify reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made.
7. Where applicable, provide to the Minister responsible for the Act:
  - a. notice of any personal information bank(s) that are in the custody or under the control of the ministry; and,
  - b. any completed privacy impact assessments or information sharing agreements to enable the Minister responsible for the Act to maintain and publish a personal information directory as required under subsections 69 (2) and (3) (b) of the Act.
8. The Minister responsible for this Act may designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative.

9. s.13

- a. whether the initiative involves personal information that is sensitive; and,
- b. if the personal information that is sensitive is disclosed to be stored outside of Canada.

Where applicable, the head of a ministry must confirm their adherence in the PIA to the following requirements under Part 3 of the Act:

10. Confirm that notice of collection will be given to individuals per section 27 (2) of the Act, or confirm that notice of collection is not required, per section 27 (3) of the Act;
11. Where personal information is used to make a decision that directly affects an individual, confirm that reasonable efforts will be made to ensure the accuracy and completeness of personal information per section 28 of the Act;
12. Confirm that a process is in place, per section 29 of the Act, to correct an individual's personal information upon request, or to annotate their personal information if it is not corrected per the individual's request;

13. Where personal information is used to make a decision that directly affects an individual, confirm that the personal information will be retained for at least one year after use, per section 31 of the Act;

**E.** s.13

1. If the conditions in D9 are not met, or the disclosure outside of Canada is made in accordance with section 33 (2) (f), an assessment of disclosure outside of Canada is not required.
2. If both conditions in D9 are met, then an assessment of disclosure outside of Canada is required and must be conducted as part of the privacy impact assessment.
3. If an assessment of disclosure outside of Canada is required, the head of a ministry must identify the privacy risk(s) as well as the level of the privacy risk(s) associated with the disclosure by examining factors which include but are not limited to the following:
  - a. the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information;
  - b. the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information;
  - c. whether the personal information is stored by a service provider; and,
  - d. where the personal information is stored.
4. For each privacy risk, identify a privacy risk response that is proportionate to the level of risk posed. These may include technical, security, administrative or contractual measures (e.g. ways to manage and review access to personal information).
5. The outcome of the assessment of disclosure for storage of personal information outside of Canada will be a risk-based decision made by the head of the ministry on whether to proceed with the initiative, considering E3 and E4.

**F. Directions on conducting a PIA for an enactment**

When conducting a PIA for a proposed enactment, including a proposed amendment to an enactment, the head of a ministry must do the following:

1. Identify the purpose or objective of the proposed enactment or amendment to the enactment.
2. For the proposed enactment or amendment to the enactment, identify:
  - a. Any provisions that will authorize the collection, use or disclosure of personal information;
  - b. What elements of information, including personal information, that will be authorized to be collected, used or disclosed;
  - c. That the personal information authorized to be collected, used or disclosed is necessary for the purpose of the initiative;
  - d. Any provisions that provide a regulation-making power with respect to the collection, use, or disclosure of personal information;
  - e. Any provisions that would override or otherwise limit the privacy protection provisions of the Act, and the rationale for such provisions; and,
  - f. Other impacts to the rights of individuals afforded under the Act.

## **G. Directions on documenting a PIA and submitting it for review and comment**

When documenting a PIA for an initiative that is not an enactment, the head of a ministry must, at a minimum, do the following:

1. Document all required elements under Sections D and E of these directions;
2. Provide sufficient detail in the documentation to enable the Minister responsible for the Act to review and comment;
3. Document the PIA using the template(s) created by the Minister responsible for the Act or in a form and manner approved by the Minister responsible for the Act; and,
  - a. Provide the name, position title, and contact information of the individual who can answer questions with respect to the PIA.

When documenting a PIA for an initiative that is an enactment, the head of a ministry must, at a minimum, do the following:

1. Document all required elements under Section F of these directions;
2. Provide sufficient detail in the documentation to enable the Minister responsible for the Act to review and comment on the PIA;

3. Document the PIA using the template(s) created by the Minister responsible for the Act or in a form and manner approved by the Minister responsible for the Act; and,
4. Provide the name and contact information of the individual who can answer questions with respect to the PIA.



## PRIVACY IMPACT ASSESSMENT DIRECTIONS

**TO:** HEADS OF ALL PUBLIC BODIES THAT ARE NOT MINISTRIES

**DIRECTION:** -

**SUBJECT:** Directions to heads of public bodies that are not ministries on conducting privacy impact assessments

**AUTHORITY:** These directions are issued under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*.

**APPLICATION:** These directions apply to heads of all public bodies that are not ministries.

**EFFECTIVE DATE:** Month Day, Year

---

Honourable Lisa Beare  
Minister of Citizens' Services

## **Minister of Citizens' Services**

### **Directions to Heads of Public Bodies that are Not Ministries issued under Section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act***

I, Lisa Beare, Minister of Citizens' Services (the Minister), issue the following directions to heads of public bodies that are not ministries, hereafter referred to as "public bodies", under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 (the Act).

These directions repeal and replace Direction 1/14 issued May 9, 2014.

#### **A. Preamble**

##### **Relevant Legislative Requirements**

Section 69 (5.3) of the Act requires the head of a ministry to conduct a privacy impact assessment (PIA) and must do so in accordance with the directions of the Minister responsible for the Act.

##### **Purpose**

The purpose of these directions is to:

1. Direct public bodies in determining when a PIA must or may be conducted.
2. Direct public bodies in conducting and documenting a PIA that will:
  - a. Determine whether their initiative meets or will meet the requirements under Part 3 of the Act; and
  - b. Identify and assess privacy risks and identify a risk response(s) that is proportionate to the level of the risk.

#### **B. Definitions**

In these directions:

“common or integrated program or activity” has the same meaning as in the Act;

“data-linking program” has the same meaning as in the Act;

“head” has the same meaning as the head of a public body that is not a ministry in Schedule 1 of the Act;

“initiative” means an enactment, system, project, program, or activity;

“ministry” means a ministry of the government of British Columbia;

“personal information” has the same meaning as in the Act;

“privacy impact assessment (PIA)” has the same meaning as in the Act;

“privacy risk” includes:

- an inherent risk of unauthorized collection, use, disclosure, or storage of personal information; and
- something that may inappropriately override or otherwise limit personal privacy.

The level of risk may vary based on:

- the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information; and
- the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information.

“public body” means a public body as defined in the Act that is not a ministry; and,

“service provider” has the same meaning as in the Act.

## **C. When a PIA must or may be conducted**

1. A head of a public body must conduct a PIA on a new initiative for which no PIA has previously been conducted.
2. s.13



3. Where a head of a public body is not required to conduct a PIA by items 1-2, above, they may conduct a PIA at their discretion and in accordance with these directions.

## **D. General Directions on conducting a PIA**

When conducting a PIA for an initiative, the head of a public body must do the following:

1. Identify the purpose or objective of the initiative.
2. Identify the information elements, including personal information, to be collected, used, disclosed, or stored, and confirm that the personal information elements are necessary for the purpose of the initiative.
3. Where applicable identify:
  - a. how and from whom the personal information will be collected;
  - b. how the personal information will be used;
  - c. how and to whom personal information will be disclosed; and
  - d. if an assessment or disclosure for storage of personal information outside of Canada is required, as per E.
4. Identify relevant legal authority (or authorities) authorizing the collection, use, or disclosure of personal information, as applicable.
5. If the initiative involves personal information, identify privacy risks and privacy risk responses that are proportionate to the identified risk.
6. Identify reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made.
7. The head of a public body may document the PIA using a template created by the Minister responsible for the Act or an appropriate format as determined by the head of the public body.
8. Designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative.

9. s.13

- a. whether the initiative involves personal information that is sensitive; and,
- b. if the personal information that is sensitive is disclosed to be stored outside of Canada.

Where applicable, the head of the public body must confirm their adherence in the PIA to the following requirements under Part 3 of the Act:

10. Confirm that notice of collection will be given to individuals per section 27 (2) of the Act, or confirm that notice of collection is not required, per section 27 (3) of the Act;
11. Where personal information is used to make a decision that directly affects an individual, confirm that reasonable efforts will be made to ensure the accuracy and completeness of personal information per section 28 of the Act;
12. Confirm that a process is in place, per section 29 of the Act, to correct individuals' personal information upon request, or to annotate their personal information if it is not corrected per the individual's request;
13. Where personal information is used to make a decision that directly affects an individual, confirm that the personal information will be retained for at least one year after use, per section 31 of the Act;

**E.** s.13

1. If the conditions in D9 are not met, or the disclosure outside of Canada is made in accordance with section 33 (2) (f), an assessment of disclosure for storage of personal information outside of Canada is not required.
2. If both conditions in D9 are met, then an assessment of disclosure for storage of personal information outside of Canada is required.
3. If an assessment of disclosure for storage of personal information outside of Canada is required, the head of a public body must identify the privacy risk(s) as well as the level of the privacy risk(s) associated with the disclosure by examining factors which include but are not limited to the following:

- a. the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information;
  - b. the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information;
  - c. whether the personal information is stored by a service provider; and,
  - d. where the personal information is stored.
4. For each privacy risk, identify a privacy risk response that is proportionate to the level of risk posed. These may include technical, security, administrative or contractual measures (e.g. ways to manage and review access to personal information).
5. The outcome of the assessment of disclosure for storage of personal information outside Canada will be a risk-based decision made by the head of the public body on whether to proceed with the initiative, considering E3 and E4.

# Questions and Answers:

## *Freedom of Information and Protection of Privacy Act Amendments*

### Contents

General Questions .....	6
Q1. Why do we need to amend FOIPPA?.....	6
Q2. Why these amendments in particular? .....	6
Q3. Which amendments increase transparency and accountability? .....	7
Q4. Why do fees need to be introduced, and how will they help?.....	8
Q5. What consultations have taken place?.....	8
Q6. Which Indigenous partners have you spoken with? .....	9
Q7. s.16 .....	10
Q8. Did you consult with advocacy groups such as the B.C. Freedom of Information and Privacy Association (FIPA)?.....	10
Q9. How does the package reflect input received through consultation and engagement? .....	11
Q10. How will the amendments address previous Special Committee and Commissioner recommendations?.....	12
Q11. Why aren't you waiting for the new Special Committee's recommendations? .....	12
Q12. Have you addressed all of the recommendation made by past Special Committees? .....	13
Q13. How will these amendments modernize services in the public sector? .....	13
Q14. How will the proposed amendments enhance privacy protections?.....	14
Q15. How will these amendments further diversity, inclusion, reconciliation and equity?.....	14
Q16. What legislative tools do we currently have in place to protect privacy? .....	15
Q17. What are the fiscal implications of these amendments? .....	16
Q18. What are the labour implications of these amendments?.....	17
Q19. When will the amendments come into force? .....	17
Q20. How will public bodies be supported in meeting their new obligations? .....	17
Removing Outdated Gendered and Non-Inclusive Language.....	18
Q1. Will these amendments address the gendered language identified by former MLA Andrew Weaver in his 2018 Private Member's Bill?.....	18
Q2. How does this relate to the Better Regulations for British Columbia Project? Is there some overlap here? 18	
Excluding Exam/Test Answers from Coverage Under FOIPPA.....	18

Q1. Why do we need to exclude exam/test answers from FOIPPA? Didn't the B.C. Court of Appeal rule on this issue already?.....	18
Ensuring "Records Available for Purchase" are Still Bound by the Act's Privacy Protection Provisions in Part 3.....	19
Q1. Aren't records available for purchase already contemplated under the Act? Why is this amendment needed?.....	19
Constraining Information Rights to Records that Relate to Public Body Business .....	20
Q1. Isn't FOIPPA already limited to records of public body business? Why is this amendment necessary?.....	20
Q2. Is anyone else in Canada doing this?.....	20
Q3. Can you provide some examples of requests that do not relate to public body business?.....	21
Q4. How will government prevent this provision from being used to avoid access requests? .....	21
Excluding Lawfully Deleted Electronic Records from FOI .....	22
Q1. Why is it necessary to exclude deleted records from Part 2 of the Act? .....	22
Q2. Won't this amendment prevent people from accessing records that are potentially responsive to their request?.....	22
Q3. Won't excluding deleted items from the scope of FOIPPA incentivize employees to retain as few records as possible? .....	23
Modernizing Business Contact Information Requirements.....	23
Q1. Are these amendments removing the requirement to provide a contact person when collecting personal information or responding to an access request? .....	23
Protecting Indigenous Information, Cultural Heritage and Relations and Negotiations with Indigenous Governments .....	24
Q1. Why are these amendments necessary?.....	24
Q2. To what extent were Indigenous nations and organizations consulted on these amendments? ...	24
Q3. Why did government remove the 15-year limitation for disclosing information related to Indigenous government relations or negotiations? .....	26
Q4. Does government expect any impacts or delays to FOI services because of this new requirement to consult Indigenous governing entities?.....	26
Protecting the Identity of a Third Party that Provided a Personal Recommendation or Evaluation or Character Reference .....	26
Q1. How will the proposed amendment better protect privacy?.....	26
Indirect Collection of Personal Information that is Disclosed Under Another Enactment.....	27
Q1. What kinds of indirect collections will this enable? Can you provide examples? .....	27
Repealing/Modernizing Data-residency Provisions .....	27
Q1. Will these amendments weaken privacy protections? .....	27

Q2. s.13	29
Q3. What about the risks posed by the U.S. Patriot Act? .....	29
Q4. Did the 2019 FOIPPA amendments (re: temporary processing) not resolve this issue? .....	30
Q5. What are other jurisdictions doing? .....	30
Q6. Australia has recently mandated that its government store its data in Australia; why is B.C. going in the opposite direction? .....	31
Q7. What happens if we don't make this change? .....	31
Q8. s.13	
Q9. Why can't we make the temporary COVID order permanent? .....	32
Q10. The Special Committee recommended retaining the Act's data-residency provisions. Why are we doing the opposite? .....	33
Enabling More Sharing of Information with Indigenous Governing Entities .....	34
Q1. Why is this amendment necessary? Doesn't the Act already have authorities in place for this kind of sharing? .....	34
Q2. What consultation has been done to inform this amendment? .....	34
Q3. Does this amendment support reconciliation? .....	35
Q4. Why has the Ministry proposed their own definition of "Indigenous governing entity" when "Indigenous governing body" is already defined in the <i>Declaration on the Rights of Indigenous Peoples Act</i> (DRIPA)? .....	36
Data Linking .....	36
Q1. Why are amendments to the Act's data-linking provisions needed? .....	36
Q2. Will these amendments enhance privacy? .....	37
Q3. Will these proposed amendments increase inappropriate information sharing by public bodies? .....	37
Q4. Will there be any exemptions? .....	37
Public Bodies Must Have a Privacy Management Program .....	37
Q1. What is a privacy management program? .....	37
Q2. Will the requirement to have a privacy management program have significant impacts, financial or otherwise, on public bodies' operations? .....	38
Q3. When do you anticipate ministerial directions will be issued? .....	38
Mandatory Breach Notification .....	39
Q1. How will this impact ministries and broader public sector? .....	39
Q2. Why is this coming into force later? .....	39
Q3. What are other jurisdictions doing? .....	39
Expanding Criteria for Commissioner to Authorize Disregarding of FOI requests .....	40

Q1. Why is it necessary to expand the Commissioner's ability to authorize a public body to disregard requests?.....	40
Q2. What evidence do we have showing that the current section 43 is not working effectively? .....	41
Q3. How frequently and in what circumstances would we expect the proposed provisions to be invoked?.....	41
Statements to the Information and Privacy Commissioner Given During an Audit are Not Admissible as Evidence .....	42
Q1. Why is this amendment necessary? .....	42
New Offence Provisions and Associated Penalties .....	42
General.....	42
Q1. Why are these new offence provisions necessary?.....	42
Q2. Why are the new offence provisions limited to wilful acts? .....	42
Q3. Can you provide a common example of a situation in which these offences would apply? .....	43
Offence Respecting Wilful Destruction.....	43
Q4. Do other jurisdictions in Canada have similar provisions regarding the wilful destruction of records to evade a request for access to information? .....	43
Q5. Why don't the proposed amendments provide the Commissioner with oversight over unauthorized destruction of government records, as per the recommendations from the Special Committee and the Commissioner? .....	44
Offences Respecting Unauthorized Collection and Use .....	44
Q6. Do other jurisdictions in Canada have similar provisions regarding the unauthorized collection and use of personal information?.....	44
Q7. What will the fine amount be for unauthorized collection and use?.....	44
Q8. Why increase the maximum offence penalties? .....	44
Strengthening Privacy Impact Assessment (PIA) Requirements.....	45
Q1. How will the updates to the Act's PIA requirements strengthen privacy? .....	45
Authorizing a Public Body to Withhold Information from a Record Released under Section 71 or 71.1...	45
Q1. Will this limit the quality or quantity of records currently disclosed without a request for access? 45	
Application Fees for General FOI Requests .....	46
Q1. s.12; s.13	
Q2. How many Canadian jurisdictions charge an application fee under their public access to information legislation? .....	46
Q3. Which Canadian jurisdictions charge the most (how much)? .....	46
Q4. What is the average application fee charged by Canadian jurisdictions? .....	47

Q5.	s.13	
s.13		
Q6.	s.13	
Q7.	What evidence is there that a small portion of applicants are monopolizing and affecting the system? .....	48
Q8.	Will an application fee help to recoup costs of processing an FOI request? .....	49
Q9.	How much does it cost government to process an FOI request? .....	49
Q10.	How many FOI requests are received per year in B.C.? .....	49
Q11.	How many general FOI requests currently generate a processing fee? .....	50
Q12.	Of the current fee estimates issued, how many fees are actually paid? .....	50
Q13.	Will the application fee be able to be waived? If not, why not? .....	50
Expanding Coverage of the Act .....		51
Q1.	Have criteria been established for adding subsidiary entities? .....	51
Q2.	Is there a list of subsidiary entities that are being considered for addition immediately? .....	51
Item 25: Remove the Reference to the <i>Hospital (Auxiliary) Act</i> .....		51
Q1.	Why is the removal of the reference to the <i>Hospital (Auxiliary) Act</i> necessary? .....	51
Removing Definition of “Social Media Site” .....		52
Q1.	Will the removal of prescribed social media sites relax the standards/safeguards for how public bodies use social media? .....	52
Q2.	Will removing “site” from the definition of “social media” leave the term open to interpretation? .....	52
Covering British Columbia Association of Chiefs of Police (BCACP) and British Columbia Association of Municipal Chiefs of Police (BCAMCP) Under FOIPPA .....		
Q1.	Will this change affect BCACP’s and BCAMCP’s ability to have frank and effective conversations about matters of public safety or law enforcement? .....	52
Office of the Premier Coverage under FOIPPA .....		53
Q1.	Is the Office of the Premier not already covered under FOIPPA under Schedule 2? .....	53
Q2.	Why is this amendment necessary? .....	53



## General Questions

### Q1. Why do we need to amend FOIPPA?

- FOIPPA has not been substantially updated since 2011, and no longer reflects the expectations and experiences of the public and others affected by it.
- We want to ensure the legislation keeps pace with new technologies, enhances privacy protection, and provides the level of service that people expect from the government.
- The changes we're proposing will strengthen government accountability and transparency by enabling us to be more responsive to the needs of people.
- These amendments will reinforce the Act's original spirit and intent, and improve B.C.'s high-quality freedom of information services by freeing up government resources to respond to people's requests faster.

### Q2. Why these amendments in particular?

- Proposed amendments to the Act will:
  - enable the B.C. public sector to provide the level of service people expect in the digital era;
  - enhance public sector privacy protections;
  - demonstrate the Province's commitments to diversity, inclusion, reconciliation and equity; and
  - clean up minor housekeeping issues in the Act, including redundancies and interpretation issues.
- Our amendments have been informed by input from the public, Indigenous leaders, businesses and organizations and will enhance our ability to respond to people's changing needs, quickly and efficiently, including improved support for diversity, inclusion, reconciliation and equity.

- Many of the amendments respond to recommendations made by the Office of the Information and Privacy Commissioner and previous Special Committees of the Legislative Assembly that reviewed FOIPPA.

Q3. Which amendments increase transparency and accountability?

- Mandatory breach notification (to individuals) and reporting (to the OIPC) will make us more accountable to individuals where their information is at risk.
- We are creating a new offence for wilfully destroying records to evade FOI, to ensure there is never another triple-delete scandal.
- New FOI protections for information that is important to Indigenous peoples will improve our accountability to our Indigenous partners and their wishes.
- We are also adding new information sharing abilities that will allow us to share more information with Indigenous governments.
- Requirements for public bodies to have privacy management programs will make them more accountable to individuals whose personal information they hold.
- Expanding the privacy offences in the Act will ensure public servants are held accountable if they wilfully encroach on someone's privacy.
- Raising the penalties for all offences will strengthen the overall accountability measures held within FOIPPA.
- Amended powers for the Minister will permit government to add subsidiary entities as new public bodies under the Act, as recommended by the Special Committee.
- Further, we are actively adding two new public bodies that will become subject to the Act – the BC Association of Chiefs of Police and the BC Association of Municipal Chiefs of Police.

Q4. Why do fees need to be introduced, and how will they help?

- People, businesses and organizations deserve to have timely access to information, and British Columbians do not get full value from the FOI system when it is inundated by a small number of applicants.
- The backlog created by a handful of high-volume requestors having a direct impact on the resources available to respond to others – such as personal requests from youth in care, inmates, and disability or income assistance requestors.
- Introducing an application fee for general FOI requests and limiting requests to public body business will improve the health of our FOI system for the benefit of all British Columbians.
- The application fee is intended to reinforce the spirit and intent of the Act by encouraging applicants to be more focused when making requests, which will free up government resources so that we can be more responsive to requests that we receive.

Q5. What consultations have taken place?

- The proposed amendments reflect what we've heard through many engagements and consultations.
- In 2018/19, substantial engagement was completed to identify stakeholder concerns and priority issues. This engagement included:
  - An online public engagement through govTogetherBC on matters related to both access to information and protection of privacy
  - A series of roundtable discussions was held by the then-Minister of Citizens' Services with key stakeholder groups.
  - Ministry staff held discussions with the Union of B.C. Indian Chiefs and the First Nations Summit on the unique impacts access and privacy have on Indigenous peoples and conducted a mail-out engagement campaign, asking for input and recommendations from over 200 First Nations

communities throughout B.C. on privacy and access to information.

- Feedback from previous stakeholder sessions, input from subject-matter experts across government, and recommendations from the OIPC and past Special Committees informed the current package of proposed amendments.
- Building on earlier consultations, the Ministry re-engaged with stakeholder groups and partners to confirm previous inputs and to gain a current understanding of potential impacts.
- The latest round of engagement took place between April and September 2021 with government ministries, broader public sector public bodies, municipalities, Indigenous groups and communities, the B.C. tech sector, the OIPC and the public.
- Feedback was received through Minister and ADM roundtable meetings, presentations to stakeholder groups, meetings with Ministry staff and two public surveys administered by govTogetherBC and Ipsos, which received 1,600 and 800 responses, respectively.

Q6. Which Indigenous partners have you spoken with?

- The Ministry has had a number of meaningful discussions with the First Nations Leadership Council. Conversations included representatives from the Union of BC Indian Chiefs, First Nations Summit and the BC Assembly of First Nations. These discussions informed and shaped a number of the proposals which specifically relate to Indigenous peoples.
- An invitation was provided to the leaders of First Nations across the province to complete an online questionnaire, which sought to gain the perspective of Indigenous people on access to information and privacy.
  - In response to this invitation, representatives from the Stk'emlupsemc Te Secwepemc (stuh-KUM-loops tay shuh-WHEP-muhk) Nation requested a meeting with Ministry staff, which was held in early September 2021.

- In addition, Deputy Minister Shauna Brouwer sent a formal invitation to leaders of the Union of BC Indian Chiefs, First Nations Summit, BC Assembly of First Nations and Metis Nation BC to discuss the proposed amendments.
- Within the established Treaty First Nations notification framework, the Ministry also engaged with representatives from the five Maa-nulth (maw-nawlth) nations, Tsawwassen (tsa-wah-sen) First Nation and the Nisga'a Lisims (nis-gah liss-ums) Government.
- All of this built on engagement done in 2018/19, when Ministry staff held discussions with the Union of B.C. Indian Chiefs and the First Nations Summit on the unique impacts access and privacy have on Indigenous peoples and conducted a mail-out engagement campaign, asking for input and recommendations from over 200 First Nations communities throughout B.C on privacy and access to information.
- In alignment with B.C.'s Declaration Act, we will continue to work in consultation and co-operation with Indigenous peoples as we move forward with this work.

s.16

Q8. Did you consult with advocacy groups such as the B.C. Freedom of Information and Privacy Association (FIPA)?

- We engaged with FIPA in 2018/19 on a similar package of amendments

- We also considered FIPA's submissions to previous Special Committees of the Legislative Assembly that reviewed the Act when developing our amendments package.
- In spring and summer 2021, we focussed on talking to directly impacted stakeholders and partners, such as public bodies, the OIPC, the public and Indigenous representatives.

Q9. How does the package reflect input received through consultation and engagement?

- Several of the proposed amendments address recommendations made during consultation.
  - For example, the amendments to s. 16 and the addition of the new s. 18.1 were developed in response to issues raised by Indigenous representatives and the natural resource ministries and validated during consultations.
- Several other significant proposals address recommendations made by stakeholders, including the OIPC, Special Committees, and access to information and privacy advocates.
- These proposals include:
  - An offence and penalty for the wilful destruction of records with the intent to evade a request for access.
  - An offence and penalty for unauthorized collection or use of personal information.
  - The expansion of coverage of the Act to include subsidiary entities owned or controlled by public bodies.
  - A new legal requirement to notify affected individuals and report to the Commissioner where a privacy breach could reasonably be expected to cause significant harm to the individual.
  - A new legal requirement for public bodies to have a privacy management program.

- The proposed amendments to the Act's data-linking provisions were developed in close consultation with the OIPC.

Q10. How will the amendments address previous Special Committee and Commissioner recommendations?

- There are many longstanding recommendations from previous Special Committees of the Legislative Assembly that reviewed the Act, and from the Information and Privacy Commissioner.
  - The proposed amendments address several of these recommendations, including recommendations about mandatory breach reporting, privacy management programs and subsidiary corporations.
- Several of their other recommendations have also been addressed through other policy instruments or mechanisms.
  - For example, FOI applicant anonymity is protected through policy.
  - And we have issued several new proactive disclosure directives in recent years to address recommendations related to government accountability and transparency.

Q11. Why aren't you waiting for the new Special Committee's recommendations?

- Aside from the 2019 minor amendments, the Act has not been substantially updated since 2011 which means many recommendations from the last two Special Committees (2010/11 and 2015/16) remain unaddressed.
- We anticipate that the new Special Committee would, if we waited to amend the Act, repeat many previous recommendations.
- Updating the Act now allows the new Special Committee to focus on emerging issues.

Q12. Have you addressed all of the recommendation made by past Special Committees?

- While all recommendations made by past Special Committees have been thoroughly reviewed, not all of the recommendations will be addressed through this package.
- Several Special Committee recommendations have already been addressed through policy, while there were a number of records management related questions satisfied through the introduction of the *Information Management Act*.
- Additionally, there are a number of recommendations which cannot be addressed through amendments to FOIPPA, such as the recommendation to enact new health information privacy law.
- **(If asked)** Of the 39 recommendations contained in the Special Committee's 2016 report:
  - 9 recommendations will be addressed through this Bill.
  - 8 recommendations have been addressed through other means such as the *Information Management Act* or government policy.
  - 22 recommendations remain unaddressed.

Q13. How will these amendments modernize services in the public sector?

- Many of the proposed amendments, particularly proposed changes to the Act's data-residency provisions, will improve how people access government services.
- This will be especially important through the continuing COVID-19 pandemic and recovery.
- The proposed amendments will help people access more government services online, which they expect now and into the future.
- The amendments will also result in important improvements to FOI services.



- People, businesses and organizations deserve to have timely access to information, and British Columbians do not get full value from the FOI system when it is inundated by a small number of applicants.
- The backlog created by a handful of high-volume requestors having a direct impact on the resources available to respond to others – such as personal requests from youth in care, inmates, and disability or income assistance requestors.
- Introducing an application fee for general FOI requests and limiting requests to public body business will improve the health of our FOI system for the benefit of all British Columbians.
- The application fee is intended to reinforce the spirit and intent of the Act by encouraging applicants to be more focused when making requests, which will free up government resources so that we can be more responsive to requests that we receive.

Q14. How will the proposed amendments enhance privacy protections?

- Many of the proposed amendments will address privacy issues and help us strengthen privacy for British Columbians. These amendments include:
  - Mandatory breach notification;
  - Requirement to have a privacy management program; and
  - Increasing maximum penalties for privacy-related offences

Q15. How will these amendments further diversity, inclusion, reconciliation and equity?

- As part of this work, we reviewed the Act through a critical Gender-based Analysis Plus (GBA+) lens.

- This showed us that there are a few things in the Act that need an update.
- Amendments have been proposed based on the principles of lasting and meaningful reconciliation, and equity and anti-racism.
- These amendments will:
  - Enable more information sharing with Indigenous governments;
  - Protect sensitive information related to Indigenous peoples to protect information that if released could harm the rights of an Indigenous people to maintain, control, protect or develop their cultural heritage; traditional knowledge; traditional cultural expressions; or manifestations of sciences, technologies or cultures.
  - Ensure that information that could harm relations with Indigenous governing entities is protected; and
  - Remove outdated and non-inclusive language from the Act.

Q16. What legislative tools do we currently have in place to protect privacy?

- FOIPPA establishes the Information and Privacy Commissioner and provides them with oversight over privacy as well as access to information.
- FOIPPA requires public bodies to complete a Privacy Impact Assessment (PIA) on proposed initiatives.
- A PIA considers risk, case by case, based on the specific activities and information involved in each initiative. This includes ensuring that the security of personal information is reasonable and commensurate with the information's sensitivity.
- One of the proposed amendments will clarify the PIA requirements for public bodies.

Q17. What are the fiscal implications of these amendments?

- These proposals are expected to result in minimal fiscal impacts to ministries given that many of the amendments will simply formalize existing business practices.
  - For example, a new legal requirement will be created respecting privacy management programs, and mature privacy management programs are already in place in all ministries.
- Proposed amendments that are expected to have fiscal implications for the broader public sector will be brought into force in phases, to provide public bodies with enough time to prepare to implement these new requirements.
  - For example, non-ministry public bodies may not have privacy management programs in place at the same level of maturity as ministries.
- Changes to the Act's data-residency provisions are expected to have positive fiscal effects across the public sector.
  - These changes will result in more competitive procurements, less being spent on the negotiation and administration of complex contracts, and more cost-effective technology that does not need expensive customization in order to meet legal requirements.
- Several of the proposals are expected to reduce the numerous bad-faith or overly broad FOI requests currently being made to ministries, which is also expected to have a positive fiscal impact.

s.12; s.13

Q18. What are the labour implications of these amendments?

- The Ministry has consulted with the Public Service Agency and does not believe there are any significant labour relations implications associated with these amendments.

Q19. When will the amendments come into force?

- These amendments will come into force upon Royal Assent, with the exception of the following:
  - The requirement for public bodies to have a privacy management program (PMPs).
    - This will give non-ministry public bodies that don't already have PMPs time to prepare to meet this new legal requirement.
  - The requirement to notify affected individuals and report to the Information and Privacy Commissioner where a privacy breach could reasonably be expected to cause significant harm.
    - Ministries are already required to do this in policy, but delaying this requirement coming into force will give non-ministry public bodies and the Office of Information and Privacy Commissioner time to prepare.
  - The addition of the BC Association of Chiefs of Police and the BC Association of Municipal Chiefs of Police.
    - This will allow these associations time to prepare to meet the Act's requirements.

Q20. How will public bodies be supported in meeting their new obligations?

- Ministry staff are working on guidance materials as well as a comprehensive training plan to support public bodies through the implementation of these new requirements.

- All public bodies, as well the public have access to the Privacy and Access Helpline, which is administered by the Ministry of Citizens' Services.

## **Removing Outdated Gendered and Non-Inclusive Language**

Q1. Will these amendments address the gendered language identified by former MLA Andrew Weaver in his 2018 Private Member's Bill?

- These amendments will ensure the Act's language reflects contemporary standards with respect to gender identity and expression.
- In addition, the amendments will also ensure the Act's language is reflective of contemporary standards regarding Indigenous identity and disability.

Q2. How does this relate to the Better Regulations for British Columbia Project? Is there some overlap here?

- The Better Regulations for British Columbia Project updated 600 instances of gendered language in the regulations of 15 ministries – including the regulations for FOIPPA and PIPA.
- The recent Better Regulations project only included gendered language in regulations, and not in legislation.
- Our proposal aligns with this project as it seeks to similarly update the outdated gendered language in the Act, and simultaneously update other non-inclusive language.

## **Excluding Exam/Test Answers from Coverage Under FOIPPA**

Q1. Why do we need to exclude exam/test answers from FOIPPA? Didn't the B.C. Court of Appeal rule on this issue already?

- There have been different interpretations of section 3(1)(d) of the Act, which excludes "a record of a question that is to be used on an examination or test" from disclosure.

- The current language does not explicitly exclude an answer to an examination or test question.
- In 2018, a decision from the B.C. Court of Appeal stated that “a record which discloses a question, either explicitly or implicitly, is included within the exclusion in s. 3(1)(d)”.
  - This supports the notion that a record that includes anything that is important to an exam question, including the answer, should not be disclosed in response to an FOI request.
- The intention of this amendment is to protect both questions and answers to exams or tests, and the change will make it clear that section 3(1)(d) applies to records that would reveal both questions and answers, whether explicitly or implicitly

### **Ensuring “Records Available for Purchase” are Still Bound by the Act’s Privacy Protection Provisions in Part 3**

Q1. Aren’t records available for purchase already contemplated under the Act? Why is this amendment needed?

- Yes. Section 3(1) was amended in 2011 to clarify that records available for purchase by the public are not covered by the Act, and, therefore, are not subject to formal access to information requests and fee waivers under the Act.
- However, the amendments unintentionally excluded them from coverage under Part 3 of FOIPPA as well, which means they are not subject to the Act’s privacy protection requirements. This amendment aims to rectify that issue.
- The amendment will support personal information being adequately protected by FOIPPA’s privacy protections, even if that information is in records available for purchase.

## Constraining Information Rights to Records that Relate to Public Body Business

Q1. Isn't FOIPPA already limited to records of public body business? Why is this amendment necessary?

- The original legislative intent of the Freedom of Information provisions of FOIPPA was to provide people with a mechanism to access government records of individual or public interest with minimal exceptions.
- Modern technology has led to an exponential increase in recorded information held by public bodies.
- Many of the records retained today are created without human intervention and reveal little or no information about the work or decisions of public bodies.
- These types of records could not have been contemplated by the legislators who created FOIPPA; however, they are subject to FOIPPA's access provisions.
- FOI applicants are increasingly requesting these types of records, which, although they may reasonably be held by an employee of a public body, have no direct relationship to the public body's operations.
- There also has been an increase in the number of FOI requests that target information associated with individual government employees.
  - This abuse of the FOI system amounts to inappropriate surveillance of government officials and public service employees.
- Providing access to a record that is wholly unrelated to the carrying out of a public function is not consistent with the spirit and intent of the Act and poses additional personal privacy risks.

Q2. Is anyone else in Canada doing this?

- Yes, New Brunswick's *Right to Information and Protection of Privacy Act* has a similar provision to what we are proposing.

- Most other jurisdictions in Canada have more latitude to simply disregard requests that are clearly unrelated to government business.
  - Many don't have to apply to their Commissioner for permission to do this.

Q3. Can you provide some examples of requests that do not relate to public body business?

- Examples of some types of requests that have become common include:
  - Screenshots of phones of named individuals, showing applications.
  - Internet browser histories of named individuals.
  - Lists of all file names and folder names located on the Desktop, My Downloads, My Documents and My Favourites folders from all electronic devices used by the Premier, Ministers, Ministers of State, and OIC appointees.

Q4. How will government prevent this provision from being used to avoid access requests?

- This amendment is not about restricting access to government records.
  - It is meant to help ensure that the FOI process is used as intended, to keep government accountable and transparent about its business.
- This provision does not limit an applicant from making a request for any record related to government business.
- If access to a record is denied for any reason, the applicant has the right to make a complaint with the Information and Privacy Commissioner.
  - The Commissioner may then investigate the matter and compel government to provide records to support their investigation.



## **Excluding Lawfully Deleted Electronic Records from FOI**

Q1. Why is it necessary to exclude deleted records from Part 2 of the Act?

- This amendment aligns with current practice because under ordinary circumstances, records such as “backups” should not be restored and searched in response to FOI requests after these records have been appropriately disposed.
- Past orders from the Commissioner have long held that backups need not be searched and retrieved because the process is too costly and time-consuming to be considered reasonable.
- This is also consistent with the spirit and intent of the Act because the original records may be requested through FOI for the duration of their lifecycles.
- It should be noted that an employee’s deleted items folder is still subject to FOI, and if an employee has reason to believe that responsive records may exist in a deleted items folder, then an adequate search for records would require them to search that folder accordingly.
- This amendment does not change what an employee is legally permitted to delete.

Q2. Won’t this amendment prevent people from accessing records that are potentially responsive to their request?

- The amendment reflects past orders of the Information and Privacy Commissioner, whose office has long held that backups should not be searched and retrieved in response to FOI requests under normal circumstances.
- Good information management practices include creating, maintaining and destroying government records according to their approved information schedules, and regularly disposing of records that are “transitory” in nature.

- Backups of records are routinely created and retained for specified periods for legal or investigative purposes. If a record exists only in backup, then that record likely was disposed of lawfully.
- However, if a request for access includes “emails sent and received from this date to this date”, for example, a search of records must include ‘deleted items’ folders. A simple search of the ‘current mailbox’ would not qualify as a thorough search for responsive records.

Q3. Won’t excluding deleted items from the scope of FOIPPA incentivize employees to retain as few records as possible?

- No. Public body employees are trained to follow good information management practices.
  - This includes retaining important records and also includes deleting records, such as transitory records, when that information no longer has business value.
- Proper information management makes it easier to find records that are responsive to FOI requests.

## **Modernizing Business Contact Information Requirements**

Q1. Are these amendments removing the requirement to provide a contact person when collecting personal information or responding to an access request?

- No. These amendments will give more flexibility by enabling a public body to provide alternate means of contact, such as an email address or a social media handle, in place of, or in addition to, a telephone number or physical address.
- These amendments will ensure that anyone who has questions about a public body's collection of their personal information or their FOI request have a means of contacting that public body that reflects current practice and technology.

## **Protecting Indigenous Information, Cultural Heritage and Relations and Negotiations with Indigenous Governments**

Q1. Why are these amendments necessary?

- Right now, section 18 of FOIPPA protects information that could reasonably be expected to result in damage to, or interfere with, the conservation of fossil sites, natural sites or sites that have an anthropological or heritage value.
- This is limited in that the provision does not sufficiently describe all aspects of information related to Indigenous knowledge or cultural heritage—for instance, information related to intangible aspects of Indigenous culture such as language, resource cultivation practices, and traditional visual and performing arts.
- The Act also does not currently give Indigenous peoples the same input regarding disclosure that is afforded to other third parties when the head of a public body intends to give access to information that could be harmful to business interests or personal privacy.
- Section 16 of FOIPPA protects information that could reasonably be expected to harm intergovernmental relations—this is intended to include relations with Indigenous governing entities.
- We've heard from Indigenous partners that the current 15-year limitation on the protection of this information creates a hesitancy to share information with the Province because potential harm can persist beyond 15 years.

Q2. To what extent were Indigenous nations and organizations consulted on these amendments?

- In 2018, Ministry staff held discussions with the Union of B.C. Indian Chiefs and the First Nations Summit on the unique impacts access and privacy have on Indigenous peoples.
- In addition, government conducted a mail-out engagement campaign, soliciting input and recommendations from 200 Indigenous communities throughout B.C.

- We have worked with the Ministry of Indigenous Relations and Reconciliation as well as<sup>s.14</sup> whose feedback informed these proposed amendments.
- In 2020/21, CITZ held a number of discussions with First Nations Leadership Council members. The input received in these discussions directly informed the language of this and other amendments which specifically relate to Indigenous peoples.
- CITZ also invited the leaders of First Nations in B.C. to provide feedback through an online questionnaire, which closed on August 15, 2021.
  - A total of 11 responses were received.
  - The majority of respondents were representatives of an Indigenous government, community or organization, while a small subset (2) were interested members of the public.
  - Participants signalled a need for changes to access to information and privacy law to improve the negotiation of agreements and treaties and enhance overall collaboration between the Province and Indigenous governments.
  - Responses also revealed a general concern about the Province inappropriately sharing personal information, as well as sensitive information respecting Indigenous cultural heritage, traditional knowledge and traditional cultural expressions.
- In the past few months, we have also had meaningful dialogues with representatives from the Maa-nulth (maw-nawlth) First Nations, the Tsawwassen (tsa-wah-sen) First Nation, the Nisga'a Lisims (nis-gah liss-ums) Government, the Tk'emlúps te Secwepemc (teh-kum-loops teh sec-wep-emc) band and the Skeetchestn (Skeet-ch-sin) band.

Q3. Why did government remove the 15-year limitation for disclosing information related to Indigenous government relations or negotiations?

- Indigenous representatives made it clear during our engagement, and in past communication with government, that the 15-year limitation of this provision is not appropriate for information related to an Indigenous governing entity, as the risk of harm persists long after 15 years has elapsed.

Q4. Does government expect any impacts or delays to FOI services because of this new requirement to consult Indigenous governing entities?

- The amendments will ensure that Indigenous communities are provided with written notice and the opportunity to make written representations to a public body if the public body intends to disclose sensitive information that relates to Indigenous cultural knowledge—a right that is afforded to other third parties such as commercial entities.
- This is consistent with the current requirements for public bodies to consult prior to giving access to records that contain personal information, business information, and information that could harm inter-governmental relations.
- This amendment is not expected to have significant fiscal or operational impacts.

### **Protecting the Identity of a Third Party that Provided a Personal Recommendation or Evaluation or Character Reference**

Q1. How will the proposed amendment better protect privacy?

- Section 22(3)(h) already protects the content of a personal recommendation or evaluation from a third party.
- However, the provision does not explicitly protect the identity of the third party that provided the information for a reference or evaluation.
- The proposed amendment will establish that a disclosure of personal information is an unreasonable invasion of a third party's personal privacy if:

- the content of the recommendation or evaluation (such as a character reference), and/or
- the identity of the third party supplying that information could be revealed.

## **Indirect Collection of Personal Information that is Disclosed Under Another Enactment**

Q1. What kinds of indirect collections will this enable? Can you provide examples?

- An example would be if a ministry entered into an Information Sharing Agreement with a public body from another jurisdiction.
- The existing language of FOIPPA permits public bodies to disclose personal information to other jurisdictions, but is unclear on permitting them to collect it from public bodies in those jurisdictions.
- This amendment would provide a clear authority for the indirect collection of personal information that aligns with existing authorities for disclosure.
- To be clear, this provision does not allow a public body to circumvent the privacy protections of FOIPPA. Public bodies must still complete privacy impact assessments before entering into agreements that deal with personal information.

## **Repealing/Modernizing Data-residency Provisions**

Q1. Will these amendments weaken privacy protections?

- The Act's current data-residency requirements require all personal information to be stored and accessed within Canada except under limited circumstances.
- This blanket protection for all personal information doesn't take into account personal information that has little to no risk of causing harm.

The level of protection needed should be commensurate with the level of risk involved.

- Outside of data residency, the Act already requires public bodies to conduct a Privacy Impact Assessment (PIA).
- The PIA process considers risk, case by case, based on the specific activities and information involved in each proposed initiative.
- This includes ensuring that the security of personal information is reasonably commensurate with the information's sensitivity.
- Under the new regulation, public bodies will be required to conduct an additional assessment of any sensitive personal information being disclosed for storage outside of Canada.
- The perception that our data is safer within the physical borders of Canada is flawed.
  - Often, because of the Act's current data-residency requirements, public bodies are forced to use services that are perhaps less secure than similar services offered by more established tech companies based abroad.
  - These larger companies have more resources to devote to data security.
  - We spend approximately \$25 million each year on information security, but the large tech firms spend over \$1 billion per year – each.
- The perception that the cloud is not safe is also flawed.
  - Cloud computing is used to house (non-critical) data belonging to:
    - The US Department of Defence
    - National Bank of Canada
    - Interpol

Q3. What about the risks posed by the U.S. Patriot Act?

- The Patriot Act is no longer in force. It has been replaced by the US Freedom Act and US Cloud Act, which pose far less risk than their predecessor because they require more targeted and specific requests that don't permit bulk data collection by law enforcement.



- The USA Freedom and Cloud acts also include a process for challenging requests that did not exist under the Patriot Act.
- Other factors play into this reduced risk, including increased automation, which reduces the number of individuals that can see information, as well as new security measures, which better protect it.
- This means that it is functionally more difficult to make legitimate law enforcement requests for B.C. data when appropriate controls are in place.

Q4. Did the 2019 FOIPPA amendments (re: temporary processing) not resolve this issue?

- In October 2019, targeted amendments to the Act were passed to enable features associated with Canadian-based cloud technology.
- These amendments permit the disclosure of personal information for temporary processing and the disclosure and storage of metadata outside of Canada, but place conditions on these disclosures to ensure privacy is protected.
- The amendments limit the use of cloud services to those that operate in Canada and otherwise meet FOIPPA's privacy protection requirements.
- These amendments have been well received, but many public bodies feel they do not go far enough.
- For example, we generally can't use Zoom or Google Docs lawfully.
- The new proposed amendments will give B.C. public bodies more latitude to use modern tools to provide modern, digital services that people need and expect.

Q5. What are other jurisdictions doing?

- With respect to disclosing personal information outside of Canada, B.C. currently has the strictest laws in the country.
- Only two other jurisdictions in Canada have data-residency provisions in legislation:

- Nova Scotia's *Personal Information International Protection Disclosure Act* contains data-residency provisions.
- New Brunswick's *Personal Health Information Privacy and Access Act* also contains data-residency requirements, but they are specific to personal health information.
- Even Europe's General Data Protection Regulation (GDPR) – widely lauded as the world's most robust privacy law – doesn't restrict data residency.

Q6. Australia has recently mandated that its government store its data in Australia; why is B.C. going in the opposite direction?

- Our Privacy Impact Assessment (PIA) process is incredibly thorough and considers risk, case by case, based on what the technology is meant to do and what data is being used for. As part of this assessment, we make sure that the security of personal information is appropriate given the sensitivity of that information.

s.13

- B.C. will still have parameters for disclosing personal information outside of Canada, but the proposed amendments will allow public bodies to take a more flexible approach based on ensuring protections are commensurate with the sensitivity of the information.

Q7. What happens if we don't make this change?

- People have come to depend on the use of a variety of tools that have been available to them through the pandemic, such as apps for virtual doctor's visits and online collaboration tools for students to learn together in a diverse environment.
- The current restrictions force public bodies to use less effective and sometimes less secure technology solutions. Our vendors are moving to

international solutions and are leaving B.C. behind without any alternatives.

- This means that, without change, public bodies in B.C. may be forced to build their own systems, at great expense, because they won't be able to access solutions on the market that comply with B.C.'s strict data-residency rules.
- Lack of access to modern tools and technologies also poses a risk to public bodies' innovation and competitiveness.
- For example, greater access to cloud-based services will improve B.C. post-secondary institutions' ability to attract students by allowing them to use many of the cloud-based education tools that their competitors can offer outside of B.C.

Q8. <sup>s.13</sup>

s.13

Q9. Why can't we make the temporary COVID order permanent?

- The current Ministerial Order enables health-care workers and other public sector staff to use tools that are not normally permitted during the COVID-19 state of emergency.
- For instance, technology has been leveraged by the Ministry of Health and Health Authorities to reduce crowding in waiting rooms and limit exposure in medical facilities through virtual medical appointment alerts (Patient Prompt), self-schedule and check-in appointments for flu shots (Waitwhile) and virtual care appointments (MyVirtual Visit).

- This order has been well received by the public sector and people in B.C., as it has temporarily enabled expanded access to modern digital communications tools, allowing government to better serve British Columbians during an incredibly challenging period.
- Although the Minister has the power to extend the Order, it can't be extended forever.
  - An amendment to the Act would avoid the need for a Ministerial Order and enable, in law, B.C. public bodies to use modern tools to provide modern, digital services that citizens need and expect.

Q10. The Special Committee recommended retaining the Act's data-residency provisions. Why are we doing the opposite?

- Amending the data-residency provisions will enable B.C. public bodies to continue to use tools to provide modern, digital services that people need and expect.
- We conducted a representative survey of British Columbians that confirmed that the priority should be about data security and online service delivery – both of which suffer as a result of data residency.
- The current restrictions force public bodies to use less effective and sometimes less secure technology solutions. Our vendors are moving to international solutions and are leaving B.C. behind without any alternatives.
- The current temporary COVID-19 Order has enabled health-care workers and other public sector staff to use tools that are not normally permitted during the COVID-19 state of emergency.
- This order has been well received by the public sector and citizens, as it has temporarily enabled expanded access to modern digital communications tools, allowing government to better serve British Columbians during an incredibly challenging period.

- We want to be able to maintain this level of service once the pandemic is over and ensure that the Act will permit us to take advantage of new technology in the future.

## **Enabling More Sharing of Information with Indigenous Governing Entities**

Q1. Why is this amendment necessary? Doesn't the Act already have authorities in place for this kind of sharing?

- Several use cases have been brought to CITZ that indicate the Act does not appropriately contemplate information sharing between the B.C. government and Indigenous governing entities in support of reconciliation activities or Indigenous self-government.
- For example, the Supreme Court of Canada's landmark Tsilhqot'in [sil-KO-tin] Nation v. British Columbia decision in 2014 resulted in Crown land becoming Aboriginal title land.
  - However, tenures and other interests that overlay those former Crown lands persist.
  - The Province is working with the Tsilhqot'in [sil-KO-tin] Nation to transition management and control of the title lands, and to collaboratively undertake enforcement and monitoring tasks.
  - In order to transition these responsibilities effectively, the Province needs to share personal information with the Tsilhqot'in [sil-KO-tin] Nation but is currently restricted from doing so by the Act.

Q2. What consultation has been done to inform this amendment?

- We have worked with the Ministry of Indigenous Relations and Reconciliation as well as Indigenous Legal Relations, whose feedback informed this proposal.

- In 2018/19, and more recently in 2020/21, CITZ held a number of discussions with First Nations Leadership Council members. The input received in these discussions directly informed the language of this and other amendments which specifically relate to Indigenous peoples.
- CITZ also invited the Indigenous leaders across B.C. to provide feedback through an online questionnaire, which closed on August 15, 2021.
  - A total of 11 responses were received.
  - The majority of respondents were representatives of an Indigenous government, community or organization, while a small subset (2) were interested members of the public.
  - Overall, responses to the questionnaire indicated that there is a desire to make it easier for Indigenous people and communities to access information held by public bodies.
- In the past few months, we have also had meaningful dialogues with representatives of meaningful dialogue with representatives from the Maa-nulth (maw-nawlth) First Nations, the Tsawwassen (tsa-wah-sen) First Nation, the Nisga'a Lisims (nis-gah liss-ums) Government, the Tk'emlúps te Secwepemc (teh-kum-loops teh sec-wep-emc) band and the Skeetchestn (Skeet-ch-sin) band.

Q3. Does this amendment support reconciliation?

- Yes. This amendment will directly support:
  - The rights of Indigenous governing entities to administer programs and manage lands and resources;
  - Negotiation of agreements and treaties between the Province and Indigenous governing entities; and
  - More effective collaboration between the Province and Indigenous governing entities in co-developing policies and programs, and in joint enforcement and monitoring activities.

Q4. Why has the Ministry proposed their own definition of “Indigenous governing entity” when “Indigenous governing body” is already defined in the *Declaration on the Rights of Indigenous Peoples Act* (DRIPA)?

- The Ministry spent a great deal of time working through this very issue. While some of our Indigenous partners expressed a desire for “Indigenous governing body” to be used in place of our proposed “Indigenous governing entity”, it was determined that “Indigenous governing body” may not be sufficiently broad.
- It was decided to include the term “Indigenous governing body” within the proposed definition of “Indigenous governing entity”.

## Data Linking

Q1. Why are amendments to the Act’s data-linking provisions needed?

- Provisions on data linking were added to FOIPPA in 2011, but they are not working as originally intended.
- The primary objective was to ensure appropriate controls were in place for data-linking initiatives.
  - This in turn was meant to ensure public bodies follow the “fair information practices” and protect the rights and interests of any affected individuals.
- Many stakeholders, including the Commissioner, feel the Act’s current data-linking provisions are confusing and difficult to apply.
- The provisions also appear to have had unintended consequences.
  - For example, the current definition does not appear to cover activities that are likely to pose increased privacy risks to individuals.
- The proposed amendments will address the inefficacy of the Act’s current data-linking provisions.

- The amendments will also ensure appropriate controls are applied to data-linking programs, which will ensure that public bodies follow the fair information practices and protect the rights and interests of individuals whose personal information is included in a data-linking program.

Q2. Will these amendments enhance privacy?

- Yes. These amendments will enable additional controls to be established through regulation for activities that pose a greater privacy risk to individuals.

Q3. Will these proposed amendments increase inappropriate information sharing by public bodies?

- No. The proposed amendments do not authorize any new information sharing.
- The proposed amendments address recommendations from the Commissioner and the Special Committee.

Q4. Will there be any exemptions?

- There will be no exemptions in the Act, but exemptions may be introduced at a later date once a regulation is established.
- (If asked)
  - The planned exemptions will include sharing within the health sector (as is currently in the legislation), as well as for law enforcement purposes, and for taxation and revenue purposes.

## **Public Bodies Must Have a Privacy Management Program**

Q1. What is a privacy management program?

- An effective privacy management program includes governance and accountability, policies and processes, and training.



- A privacy management program ensures that public bodies have the necessary framework in place to meet their privacy obligations under the Act.
- Ministries are already required, through policy, to have a privacy management program
- This amendment will set that obligation in law and extend it to the broader public sector.
- The amendment will also enable the minister responsible for the Act to issue directions on privacy management programs.

Q2. Will the requirement to have a privacy management program have significant impacts, financial or otherwise, on public bodies' operations?

- This requirement will be brought into force by regulation at a later date in order to give non-ministry public bodies more time to prepare for this obligation.
- The ministerial directions will be broad and flexible enough to promote compliance while allowing public bodies to scale the program to meet their specific needs.
- The Ministry will consult with public bodies while developing the ministerial directions to ensure that the new requirements do not have significant negative impacts on public bodies' operations.
- The Ministry will also develop guidance and training to support public bodies in meeting their obligations.

Q3. When do you anticipate ministerial directions will be issued?

- We expect to be ready to issue ministerial directions on privacy management programs in approximately one year.
- The Ministry will consult with public bodies while developing the ministerial directions to ensure that the new requirements do not have significant negative impacts on public bodies' operations.

## **Mandatory Breach Notification**

Q1. How will this impact ministries and broader public sector?

- Currently, there is no legislated requirement for public bodies to notify affected individuals or the Commissioner in the event of a privacy breach.
- Within ministries, current practice is to notify affected individuals and to report privacy breaches to the Commissioner when significant harm can be reasonably expected to occur.
- The requirement to notify and report a privacy breach would make current policy and best practice mandatory for both ministries and the broader public sector.
- This will benefit the public by enhancing accountability and transparency of ministries and the public sector.
- It will also help mitigate serious fallouts of privacy breaches.

Q2. Why is this coming into force later?

- This requirement will be brought into force by regulation to provide the broader public sector time to prepare for this new obligation.
- Government intends to bring this item into force one year after royal assent, in order to provide public bodies the opportunity to prepare for this requirement.

Q3. What are other jurisdictions doing?

- Six Canadian provinces and territories have privacy breach notification and/or reporting requirements in their public sector privacy legislation.
- Quebec's proposed Bill-64 includes these requirements.
- Ontario added mandatory breach notification requirements in 2020 that apply to various data-integration units.

- Our proposed new mandatory breach reporting requirements also align with the European Union's General Data Protection Regulation (EU GDPR).

## **Expanding Criteria for Commissioner to Authorize Disregarding of FOI requests**

Q1. Why is it necessary to expand the Commissioner's ability to authorize a public body to disregard requests?

- Section 43 of the Act permits the Commissioner to authorize the head of a public body to disregard a request that would unreasonably interfere with the public body's operations, or that is frivolous or vexatious.
- However, the current criteria are too narrow to address the unreasonable interference with public bodies' operations and abuse of access rights that have unfortunately become more and more common.
- For example,
  - Requests made by former employees of public bodies for records related to former colleagues and managers that are clearly meant to be damaging and disruptive.
  - Repeated bad-faith requests from individual FOI applicants who are unsatisfied with the response received on an initial request and proceed to target individual public servants who processed the initial request with requests for their emails, calendars, Oaths of Employment, offer letters, etc.
  - Requests made to all ministries for all emails sent to or received from a specified non-government email address, including Cc's and Bcc's, for a specified period.
- Requests of this nature are being submitted with increasing frequency by a small number of FOI applicants, and they reduce the capacity of public bodies to provide service to other FOI applicants.
- This amendment will give the Commissioner more leeway by establishing additional grounds to authorize public bodies to disregard FOI requests.

- For example, the amendment would enable the Commissioner to authorize a public body to disregard an overly broad FOI request (e.g., a request made to all ministries for all emails sent to or received from a specified non-government email address, including Cc's and Bcc's).
- This is one of several proposed amendments that will help improve the FOI system for the benefit of all applicants.

Q2. What evidence do we have showing that the current section 43 is not working effectively?

- Section 43 approval is rarely requested or obtained (approved approximately 10 times in the past 10 years) because the existing criteria is too narrow to address the unreasonable interference with public bodies' operations and abuse of access rights that have become more common.
- Because the expectation of success is so low under the current provision, many instances of system abuse are not brought forward to the OIPC for consideration.

Q3. How frequently and in what circumstances would we expect the proposed provisions to be invoked?

- While section 43 requests may increase somewhat with the expanded criteria, this provision will continue to be used only when applicants are clearly abusing access rights or when the operations of a public body are significantly impeded.
- While we don't anticipate this section will be used a lot in the future, the amendment will expand the circumstances where it could be applied.
- Commissioner approval will continue to be required for section 43 to be invoked.
- Applying the proposed expanded criteria should help curb frequent misuse of FOIPPA's access rights by a small number of applicants, which would free up public body resources and increase their capacity to provide services to other applicants and the public.

## **Statements to the Information and Privacy Commissioner Given During an Audit are Not Admissible as Evidence**

Q1. Why is this amendment necessary?

- This amendment will allow for a measure of consistency within the existing provisions respecting the powers of the Information and Privacy Commissioner.
- Currently, any statement or answer provided to the Commissioner during an investigation or an inquiry is inadmissible as evidence in court (or any other legal proceeding). This amendment will make this true for information provided during an audit as well.
- This will support the Commissioner's ability to have frank and open discussions with interviewees during audits.

## **New Offence Provisions and Associated Penalties**

### General

Q1. Why are these new offence provisions necessary?

- These new provisions respond to recommendations made by the 2015/16 Special Committee of the Legislative Assembly that reviewed FOIPPA, the Commissioner, and other stakeholders.
- These new provisions will enhance accountability and strengthen public confidence in the FOI system and privacy protection, and will encourage compliance with the Act.

Q2. Why are the new offence provisions limited to wilful acts?

- Our provision respecting the wilful destruction of records aligns with recommendations from the 2015/16 Special Committee and former Commissioner David Loukidelis to make it an offence to destroy records with the intention of denying access rights under FOIPPA.
- Limiting the offence provision respecting the destruction of records to wilful acts is intended to ensure that employees are not punished when they're managing their records in good faith.

- The provision targets only “wilful” acts of destruction for the purpose of evading a request for access to records.
- Similarly, the new offences respecting unauthorized collection and use of personal information are intended to ensure incidents of an unintentional or accidental nature are not penalized.

Q3. Can you provide a common example of a situation in which these offences would apply?

- These offences would apply in cases where someone has knowingly and intentionally contravened FOIPPA.
- They would not apply to acts committed by accident, without knowledge, or in good faith.
- For example, a government employee who, in the course of their work, inadvertently searches the wrong name in a database would not be charged under these new offences.
- Government expects these offences to apply only in rare and exceptional cases.
- Employees will not be discouraged, for example, from appropriately disposing of transitory and obsolete records for fear of committing an offence.

#### Offence Respecting Wilful Destruction

Q4. Do other jurisdictions in Canada have similar provisions regarding the wilful destruction of records to evade a request for access to information?

- Yes, eight other provinces, as well as the Yukon and the federal government, have similar provisions where the wilful destruction of records with the intent to evade an access to information request is an offence in their freedom of information legislation.

Q5. Why don't the proposed amendments provide the Commissioner with oversight over unauthorized destruction of government records, as per the recommendations from the Special Committee and the Commissioner?

- Government's position is that oversight over the destruction of government information, including unauthorized destruction, rests with the Chief Records Officer under the *Information Management Act* (IMA).
- Government's position is consistent with frameworks of other provinces and territories, which do not provide their Information and Privacy Commissioner (or equivalent position) with oversight over records and/or information management.

#### Offences Respecting Unauthorized Collection and Use

Q6. Do other jurisdictions in Canada have similar provisions regarding the unauthorized collection and use of personal information?

- Yes, seven other provinces and all three territories have similar provisions in their public sector privacy legislation.

Q7. What will the fine amount be for unauthorized collection and use?

- The existing offence scheme for these offences is currently as follows:
  - in the case of an individual, other than an individual who is a service provider, to a fine of up to \$50 000; and
  - in the case of a service provider, including a partnership that or an individual who is a service provider, to a fine of up to \$50 000, and in the case of a corporation, to a fine of up to \$500 000.

Q8. Why increase the maximum offence penalties?

- These increases respond to recommendations made by the 2015/16 Special Committee of the Legislative Assembly that reviewed FOIPPA, the Commissioner, and other stakeholders.

- The proposed amendments will simplify the Act's fine schema by raising the maximum fines for individuals and service providers to \$50,000 for all offences.
- Raising fines for individuals and service providers to \$50,000 also aligns B.C. with Saskatchewan and Manitoba.
- Higher fines are expected to further deter persons from committing offences under FOIPPA.

### **Strengthening Privacy Impact Assessment (PIA) Requirements**

Q1. How will the updates to the Act's PIA requirements strengthen privacy?

- The current wording of the provisions respecting Privacy Impact Assessments (PIAs) can be interpreted to mean public bodies do not always have to do PIAs.
- The intent of the provision has always been for all public bodies to do PIAs on any proposed system, project, program or activity.
- The amendments will give public bodies more clarity around their privacy obligations.

### **Authorizing a Public Body to Withhold Information from a Record Released under Section 71 or 71.1**

Q1. Will this limit the quality or quantity of records currently disclosed without a request for access?

- No. This amendment provides certainty with respect to current practice.
- Section 70 permits the head of a public body to sever information from a record that they would be entitled to refuse to disclose in response to a request for access, but sections 71 and 71.1 do not.
- The directives issued to date by the minister responsible for the Act already require ministries to do this when applying sections 71 and 71.1.



- For transparency, when such information is deleted, the disclosed record must include a statement of
  - the fact that information has been deleted, and
  - the reason for the deletion.

## **Application Fees for General FOI Requests**

Q1. s.12; s.13

s.12; s.13

Q2. How many Canadian jurisdictions charge an application fee under their public access to information legislation?

- Four provinces (Alberta, Ontario, PEI and Nova Scotia), Nunavut and the federal government charge application fees for general access to information requests.
  - In addition, Saskatchewan charges for access to information requests made to local governments.
- Ontario is the only jurisdiction that charges an application fee for personal information requests.

Q3. Which Canadian jurisdictions charge the most (how much)?

- Nunavut charges a \$25 application fee for general requests.

- Alberta charges \$25 for a one-time general request and \$50 for continuing general requests.

Q4. What is the average application fee charged by Canadian jurisdictions?

- The average application fee across Canada is \$5 (which includes the federal government and those jurisdictions that charge no application fee).
- Across Canada, application fees for general information requests range from \$5 to \$50.
- The federal government, along with the provinces of Ontario, Prince Edward Island (PEI) and Nova Scotia all charge a \$5 application fee for general requests.

Q5. <sup>s.13</sup>  
s.13

s.13

s.13

Q6. s.13

● s.12; s.13

s.13

Q7. What evidence is there that a small portion of applicants are monopolizing and affecting the system?

- Government processed the following number of requests in 2020/21 from the top 2 most prolific applicants:

- 1 Political Party requestor: 4,772 (\$14.3 million)
- 1 Media requestor: 397 (\$1.2 million)
- Compared to 328 (\$1 million) from all other media requestors combined
- British Columbians do not get full value from the FOI system when a small number of applicants inundate the system.
- The backlog created by a handful of prolific requestors has a direct impact on the resources available to respond to others – such as personal requests from youth in care, inmates, and disability or income assistance requestors.

Q8. Will an application fee help to recoup costs of processing an FOI request?

- No. Application fees are not intended to recover the full cost—or even a significant portion of the costs—of operating an access to information program.
- With or without fees, FOI is considered a justifiable expense because it enhances democratic governance and maintains accountability, integrity and efficiency in public bodies’ work.

s.13

Q9. How much does it cost government to process an FOI request?

- As of spring 2019, the average cost of processing a single FOI request was \$3,000. (*Source: Deloitte “Freedom of Information Process Review” report.*)

Q10. How many FOI requests are received per year in B.C.?

- In FY 2020/21:
  - Government processed and closed 10,839 FOI requests (cost to government was approximately \$32.5 million).
  - 3,691 were personal requests, where fees would not apply (cost to government was approximately \$11 million).

- 7,148 were General Requests, where application fees could be applicable (cost to government was approximately \$21.4 million).
- Over the previous 3 fiscal years, government has processed an average of 11,842 FOI requests annually.

Q11. How many general FOI requests currently generate a processing fee?

- Of the 22,680 general requests received by government in the previous three fiscal years:
  - Approximately 13%, resulted in a fee estimate being sent to the applicant.

Q12. Of the current fee estimates issued, how many fees are actually paid?

- Of the 22,680 general requests received by received by government in the previous three fiscal years:
  - Only 400, or approximately 2%, resulted in a fee being paid.
  - The total amount of fees paid, on files estimated to cost government approximately \$68 million to process, was approximately \$163,800.

Q13. Will the application fee be able to be waived? If not, why not?

- No. The cost of processing a fee waiver would negate any potential benefit derived from a modest application fee.
- s.12; s.13
- No fees are being proposed for people requesting their own personal information.

## Expanding Coverage of the Act

Q1. Have criteria been established for adding subsidiary entities?

- Yes. The proposed amendment will permit the minister responsible for FOIPPA, myself, to add under the coverage of the Act any agency, board, commission, corporation, person, office or other body that meet the following criteria:
  - any member, director or officer appointed by or under the authority of the Lieutenant Governor in Council or a minister;
  - a controlling interest in the share capital is owned by the government of British Columbia or any of its agencies or a public body; or
  - performs functions under an enactment.
- The proposed amendments will also enable the Minister responsible for FOIPPA to add an agency, board, commission, corporation, office or other body to Schedule 2 of the Act if the Minister considers it in the public interest to do so.

Q2. Is there a list of subsidiary entities that are being considered for addition immediately?

- No. We are delaying adding any subsidiary entities pending further consultation with the broader public sector and the OIPC.
- The OIPC has recommended a number of entities for inclusion under the Act, and these organizations will be evaluated for inclusion in the future.

## Item 25: Remove the Reference to the *Hospital (Auxiliary) Act*

Q1. Why is the removal of the reference to the *Hospital (Auxiliary) Act* necessary?

- A consequential amendment to FOIPPA was included in the 1999 bill repealing the *Hospital Auxiliary Act*; however, this change was never reflected in FOIPPA.

- The proposed amendment will ensure that the definition of a “health care body” is accurate and up to date.

## **Removing Definition of “Social Media Site”**

Q1. Will the removal of prescribed social media sites relax the standards/safeguards for how public bodies use social media?

- This change takes a more common-sense approach to defining social media – but it will not change how government uses social media (i.e., for promotion and public discussion).
- Public bodies that use social media as a means of engaging the public are still required to complete a Privacy Impact Assessment and will still need to meet applicable security requirements.
- Government has also issued guidelines for social media use.

Q2. Will removing “site” from the definition of “social media” leave the term open to interpretation?

- No. The term “social media” has matured enough that the term is now consistently understood.
- This amendment will provide more flexibility for public bodies that use social media to engage with the public, as public bodies will not be limited to using only those platforms identified in the regulation.

## **Covering British Columbia Association of Chiefs of Police (BCACP) and British Columbia Association of Municipal Chiefs of Police (BCAMCP) Under FOIPPA**

Q1. Will this change affect BCACP’s and BCAMCP’s ability to have frank and effective conversations about matters of public safety or law enforcement?

- No. Currently, the public is able make requests for records respecting the BCACP and the BCAMCP through individual police detachments. This amendment will simply allow FOI applicants to make requests directly to the associations themselves.

- This amendment will be brought into force through regulation at a later date to allow these police associations the time to prepare to meet their obligations under the Act.

## **Office of the Premier Coverage under FOIPPA**

Q1. Is the Office of the Premier not already covered under FOIPPA under Schedule 2?

- Yes, the Office of the Premier is currently listed in Schedule 2 as a public body.

Q2. Why is this amendment necessary?

- Some requirements apply differently to ministries than to non-ministry public bodies.
- In practice, the requirements of the Act that apply to ministries differently than to non-ministry public bodies have been considered to apply to the Office of the Premier.
- However, the presence of the Office of the Premier in Schedule 2 creates uncertainty with respect to whether the Office of the Premier is a ministry.
- This amendment will make explicit that the operations and function of the Office of the Premier are reflected in its classification as a government ministry.



Page 132 of 166 to/à Page 139 of 166

Withheld pursuant to/removed as

s.12

## **What's changing with FOIPPA, and why?**

- People's lives have changed. The COVID-19 pandemic changed the way we live, work, connect with loved ones and access the services we need.
- B.C.'s outdated *Freedom of Information and Protection of Privacy* legislation, last updated a decade ago, is not working for people.
- Through the COVID-19 pandemic, B.C. found a better, faster, more effective way to deliver the services people have come to expect.
- People want timely access to their personal information as well as to healthcare, education tools and the technology that's making their lives easier.
- Today, people can safely and securely access telehealth from home, talk to their doctor via Zoom, learn online, meet with their coworkers and do business, faster.
- Highlights of the proposed amendments include:
  - Updating data-residency provisions so public bodies such as universities or health authorities can use modern tools while continuing to protect the personal information people trust us with.
  - Strengthening public-sector privacy protections and increasing accountability by implementing mandatory privacy breach reporting and increasing penalties for offences.
  - Introducing a modest fee for non-personal FOI requests.
  - Demonstrating the Province's commitment to diversity, inclusion, reconciliation and equity by increasing information sharing with Indigenous peoples, adding cultural protections and removing non-inclusive language.

**Why changing data residency requirements is the right thing to do:**

- We listened and learned from the public, Indigenous leaders, businesses and organizations through extensive consultation over several years on FOIPPA.
- Organizations like universities, health authorities and tech companies repeatedly told us that our data residency rules were outdated.
- They stopped them from being competitive or most importantly, responsive to people's evolving needs.
- It's our role as your government to listen to what's going on in people's lives and adapt – that's why we're proposing these amendments.
- Today, people can **safely and securely** access telehealth from home, talk to their doctor via Zoom, learn online, meet with their coworkers and do business, faster.
- People want access to healthcare, education opportunities and the technology that is making their lives easier through COVID.
- The order making these advancements possible expires at the end of this year.
- We need to do the work today, to deliver the services people deserve.
- We won't go backwards -- we must move forward, together.
- Thousands of people, businesses, Indigenous groups and organizations provided input through extensive consultation over several years.
- The amendments reflect that important input and those perspectives.

**What about people's health data? Can you promise it will be safe?**

- People's data will continue to be safe and protected with these proposed amendments.
- This FOIPPA change will align data residency requirements, creating consistency across the health sector and providing opportunities to store data with greater security.
- Now, healthcare providers will be able to access to more specialized diagnostic testing tools outside the country.
- Patients will also have access to more tools to help them manage their healthcare with better security to keep their data safe.
- People can safely and securely access telehealth from home or talk to their doctor via Zoom: services that are making people's lives easier through COVID.
- None of that was possible under the old legislation, and the order making these advancements possible expires at the end of this year.
- We learned from the pandemic that we can safely make these changes.
- It's important to remember that your information is safe, no matter where it is stored and that it's protected by many layers of protection and encryption.
- Data residency doesn't protect information – effective privacy controls protect information.
- And because of the Act's current data-residency requirements, often public bodies are forced to use services that are possibly less secure than those offered by established tech companies based abroad.
- The amendments don't change government's need for Canadian datacentres. Where our service providers have Canadian options, we will opt for those.
- The Patriot Act in the US does not pose the same risks it did when data residency was first added to the Act. Technology evolution, new protections and legislation replacing the Patriot Act have all resulted in less risk.

### **What about the privacy Commissioner's concerns?**

- My staff and I have met with the Commissioner 20 times.
- We value the meaningful consultation that has occurred with the Commissioner.
- We have included many items in this package that respond directly to recommendations made by the Commissioner
- We have also revised items in response to his feedback.
- The OIPC is an independent office and is meant to be an advocate for privacy and access.
- As government, we need to balance his concerns with the concerns of others, including those of public bodies.

### **If asked about openness and transparency**

- This government is committed to transparency and accountability; you only have to look at my mandate letter to see that one of my main priorities as Minister of Citizens' Services is to provide even greater accountability to the people of this province.
- In fact, this government was the one who saw the need for greater transparency and accountability for British Columbians, nearly three decades ago.
- In 1993, we were the ones who enacted the FOIPPA legislation to hold current, and future, governments accountable to the people who trust them to make decisions on their behalf and to act with integrity.
- And today, we continue this tradition in culture and in practice, through:
  - Insisting on more proactive disclosures of information that the public can access for free. Just last week, we released each Minister's estimates binder, arguably the most crucial document to government's priorities and decision-making.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- Increasing the number of data sets open to the public. In 2017, there were 2,700 and today we are closing in on 3,200 data sets available to people, organizations and media.
- BC has also begun to proactively publish information on integrated data projects underway in BC's data innovation program.
- Our Premier sets the tone as an example for us all, making himself available for weekly availabilities with media, a public platform that encourages openness and transparency between government and members of the media who help hold us accountable.
- We're also consulting with the people of this province, often and more in-depth, than any government before us because the policies that we set in place must reflect the perspectives and input of the people of BC. In fact, in the last four years since we took office, we have embarked on 244 consultation projects, compared to the last four years of the previous government, almost half that.
- Here is the summary of the transparency items added through FOIPPA:
  - Adding ministerial power to add subsidiary entities as new public bodies
  - Requiring mandatory breach reporting to the potentially harmed individual
  - Requiring mandatory breach reporting to the Commissioner
  - Adding requiring for privacy management programs, which may include transparency measures (e.g. posted privacy policy)
  - Adding a new offence for wilfully evading FOI
  - Increasing public bodies' ability to disclose to Indigenous governing entities
  - Requiring public bodies to seek consent from Indigenous governing entities in order to disclose information that is culturally sensitive through FOI
  - Increasing transparency consistency across ministries when severing proactively disclosed records
  - Adding two new public bodies (BC Assoc of Chiefs of Police; BC Assoc. of Municipal Chiefs of Police).

**What is the rationale behind implementing fees for FOI requests?**

- The proposed application fee for non-personal requests is designed to get people the information that they deserve, faster and more efficiently.
- Because although we've increased BC's on-time FOI response rate significantly, we're hearing from people that it's taking too long to respond.
- This is mostly because of overly broad requests that are slowing down the system.
- Application fees are a tool that other jurisdictions use to deliver more efficient FOI services.
- A small fee encourages requesters to focus and streamline their requests.
- And remember, for the thousands of people in B.C. requesting their own personal information each year, there will continue to be no fee.

**If pressed on how much it will be:**

- The proposed amount will be decided through regulation.
- Fees in other jurisdictions across Canada range from \$5 - \$50 and I am recommending a fee amount within that range.

**If asked about the breakdown of fees charged:**

- The proposed application fee will not likely impact 98% of all FOI requestors.
- Of the remaining 2% of respondents, by far the most impact would be for the top 2 requesters who submit more than 4500 requests annually costing more than \$14M or half the cost of the FOI program annually.
- For all FOI requests, including both personal and non-personal requests:
  - 77% make a single request and
  - 21% of people make five or less requests a year.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- And 85% of requests that result in a search fee, are dropped after hours of time and resources spent to identify records and provide a fee estimate. 15% proceed when there is a fee estimate.

For all requests received in 2020/21 (fiscal impact is coming):

- 3,994 unique applicants
- 77% of applicants submitted only 1 request
- 90% of applicants submitted 2 or fewer requests
- 95% of applicants submitted 3 or fewer requests
- 97% of applicants submitted 4 or fewer requests
- 98% of applicants submitted 5 or fewer requests
- Only 32 applicants submitted 10 or more requests
- Only 11 applicants submitted 20 or more requests
- Only 3 applicants submitted 50 or more requests
- Only 2 applicants submitted 100 or more requests
- The top two applicants combined submitted nearly 4,500 requests

Focus only on non-personal requests, the numbers for 2020/21 look like this:

- 964 unique applicants
- 66% of applicants submitted only 1 request
- 81% of applicants submitted 2 or fewer requests
- 88% of applicants submitted 3 or fewer requests
- 92% of applicants submitted 4 or fewer requests
- 94% of applicants submitted 5 or fewer requests
- Only 25 applicants submitted 10 or more requests
- Only 8 applicants submitted 20 or more requests
- Only 2 applicants submitted 50 or more requests
- Only 2 applicants submitted 100 or more requests
- The top two applicants combined submitted nearly 4,500 requests



**How does this support Indigenous relationships and service delivery?**

- FOIPPA isn't working for people anymore, and we're making these changes based on what we've heard from extensive consultation with thousands of people, Indigenous leaders, communities and groups, organizations and businesses.
- We are creating new powers to share information with Indigenous governments
- We are adding new protections to Indigenous peoples' sensitive cultural information.
- We are removing the 15-year limit on the existing protections where information may harm an Indigenous government.
- We are also removing outdated language in reference to Indigenous partners.
- We must work together to remove barriers and ensure an improved relationship between governments.
- In alignment with B.C.'s Declaration Act, we will continue to work in consultation and co-operation with Indigenous Peoples as we move forward with this work.

**If asked about long outstanding FOI requests:**

- Our intention is to always respond within the legislative timelines.
- Some requests take longer because they may contain personal information that would be harmful to release, or it needs to be reviewed by third parties to prevent harms.
- Those steps need to happen in order to fulfill our duty to protect people's privacy.

**If asked about a specific ministry's outstanding requests ie Health:**

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- While I can't speak to specific FOIs, some requests take longer to process simply because of the nature of the information and because of the multiple layers of review that are necessary to prevent harms if released.
- Our intention is to always respond within the legislative timelines.

**Why can't you just put a cap on the number of free requests?**

- A cap system on the number of free requests is not an effective solution.
- A cap system could encourage applicants with large numbers of requests to create multiple 'usernames and contact details' to avoid being charged a fee.
- For this reason, other jurisdictions have not pursued this approach.
- By implementing an application fee, we can cut down on broad, vexatious or "fishing" requests and focus resources on people who are asking for the information that they need.

**How are you modernizing the legislation with these changes?**

- The volume of Freedom of Information (FOI) requests to the Province of British Columbia has grown substantially, and requests are more complex to resolve as new digital platforms generate new types of government records.
- Beginning June 2021, the Ministry of Citizens' Services committed \$5.3M to modernize the process to manage the 12,000 to 13,000 Freedom of Information (FOI) requests the Province receives annually.
- The FOI Modernizations Project demonstrates the Province's commitment to decrease average processing days for FOI requests from 49 to 30 days.
- The FOI Modernization Project will improve business processes as needed and build a new software system to increase efficiencies when responding to the growing number of FOI requests.
- Planned improvements include:
  - Automating routine administrative tasks related to managing requests, such as tracking, notifications and correspondence.
  - Eliminating or improving business processes to lower response times.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- Software tools to help staff speed up the analysis of the thousands of pages of records related to requests.
- The project has already delivered a software tool to automate removing duplicate records in a request, which is estimated to save over 400 hours annually. This speeds up request response as staff do not need to review duplicates of the same record.

**If asked about data residency requirements and keeping people's data safe?**

- In 2004, B.C. increased data residency controls and no other province followed our lead on that.
- The Act's current data-residency requirements require all personal information to be stored and accessed within Canada except under limited circumstances.
- This blanket protection for all personal information doesn't take into account personal information that has little to no risk of causing harm.
- The level of protection needed should be aligned with the level of risk involved, and right now it is not.
- Under the new regulation, public bodies will be required to conduct an additional assessment of any sensitive personal information being disclosed for storage outside of Canada.
- Often, because of the Act's current data-residency requirements, public bodies are forced to use services that are perhaps less secure than similar services offered by more established tech companies based abroad.
- These larger companies have more resources to devote to data security.
- We spend approximately \$25 million each year on information security, but the large tech firms spend over \$1 billion per year – each.
- Data residency doesn't protect information – effective controls protect information.

**If asked about removal of Office of the Premier from Schedule 2:**

- The Commissioner suggests there is no harm in the Premier's Office being a Schedule 2 public body – this is not the case.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- Being a ministry, and not a schedule 2 body, means that the Premier's Office is subject to higher level of scrutiny and accountability
- This amendment makes it clear that our many proactive disclosure directives apply to the Premier's Office – including for ministers' travel receipts, ministers' calendars and more.
- Essentially, this change is a clarification of legal language.
- The Premier's Office was under the list of public bodies that are not ministries and therefore officially subject to different rules under the legislation. However, they've always been treated as a ministry, and this change reinforces that.
- The Premier is considered the First Minister, and the Office of the Premier the ministry of the first minister. It is treated as such under BC's Constitution Act and elsewhere.
- Removing the Office of the Premier from Schedule 2 will clarify that they are subject to requirements under the Act that reference "ministries" and not those that reference "a public body that is not a ministry" – the former being the higher standard (e.g. for doing privacy impact assessments under 69(5)).
- Applicants may direct access requests to the Office of the Premier and using the online form will still be able to select "Office of the Premier".

**If asked about MLA Stone's assertions regarding Social Media/Data Linking:**

- This bill does not increase the amount of data linking permitted in any way.
- This bill expands the criteria to capture more initiatives such as data linking and subject those initiatives to additional oversight.
- This bill does not change what information can be collected/used/disclosed on social media.
- The only change with respect to social media is to remove the definition – because the current definition requires social media sites to be listed and lists outdated platforms like MySpace.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- Government does not scrape data from social media sites – government uses social media to enable public discussion or sharing information.
- Government has removed the requirements to submit data linking PIAs to the Commissioner on the recommendation of the OIPC – an effort to modernize their oversight model.

CONFIDENTIAL ADVICE FOR MINISTER  
**Key Messages / Topic Scripts / Questions and Answers**  
**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**  
**October 21, 2021**

---

## Questions and Answers

### 1. Why are you amending the *Freedom of Information and Protection of Privacy Act*?

- B.C.'s *Freedom of Information and Protection of Privacy Act* has not been substantially changed since 2011.
- Through the pandemic, B.C. found a better, more effective way to deliver services.
- It's our role as your government to listen to what's going on in people's lives and adapt – that's why we're making significant changes to:
  - provide the level of service that people and organizations expect,
  - keep pace with new technology,
  - ensure timely access to information for people, and
  - strengthen privacy protection.
- The proposed amendments will enhance our ability to respond to people's changing needs quickly while strengthening protections. Highlights include:
  - Updating data-residency provisions so public bodies can use modern tools while continuing to protect the personal information people trust us with. The data is encrypted with multiple layers of protection, ensuring mine and your information is safe in the cloud.
  - Strengthening public-sector privacy protections and increasing accountability by implementing mandatory privacy breach reporting and increasing penalties for offences.
  - Introducing a modest fee for non-personal FOI requests.
  - Demonstrating the Province's commitment to diversity, inclusion, reconciliation and equity by increasing information sharing with Indigenous peoples, adding cultural protections and removing non-inclusive language.
- These amendments will reinforce the Act's original spirit and intent and improve B.C.'s high-quality freedom of information services to respond to people's requests faster.

### 2. People are already learning online, accessing telehealth from home and seeing their doctors online, so why do we need these amendments?

- The pandemic taught us better ways of doing things, making everybody's lives a little bit easier through access to online healthcare, education opportunities and technology.
- Today, people can safely and securely access telehealth from home, talk to their doctor via Zoom, learn online, meet with their coworkers and do business, faster.
- The order making these advancements possible expires at the end of this year.
- We need to do the work today, to deliver the services people deserve.
- We won't go backwards -- we must move forward, together.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

**3. Your government says they are open and transparent, and making life more affordable. How can you say that when you're putting barriers between people and their right to information?**

- It's our role as your government to listen to what's going on in people's lives and adapt – that's why we're proposing these amendments today, and not waiting.
- We are a government that's focused on transparency, that's why we've increased our proactive disclosures and have committed to updating FOIPPA.
- We're making it easier and faster for people to access their information.
- Under the old legislation, people waited too long for the information they deserve because of a small number of requestors whose broad and often vexatious requests for information were slowing down the system.
- The volume of requests has increased by more than 40% over a two-year period, reaching an all-time high of over 13,000 requests in 2019/20 (13,055).
- Adding a fee to non-personal FOI requests is in line with other jurisdictions in Canada. It wasn't a barrier to information elsewhere and it won't be here in B.C.
- The fee will apply to only those requesting non-personal requests – mostly to the top 2% of frequent requestors.
- Those asking for personal information will not pay a fee at all.

**DATA-RESIDENCY: PRIVACY PROTECTION**

**4. B.C.'s privacy commissioner complained about x, y and z. What are you doing to address his concerns? For Minister: SEE SEPARATE TABLE for OIPC Summary of concerns**

- We wouldn't be introducing these amendments today if it weren't for the expert advice and guidance by the OIPC.
- Through more than a dozen meetings, we worked together with the OIPC on these proposed amendments.
- His input and perspective is integral to getting these right, for the people of B.C.
- It's important to remember that people's data is safe no matter where the data is stored.
- We have protections in place with companies to protect your information, and data is encrypted in multiple layers when stored in the cloud.

**5. The OIPC says you are stripping B.C.'s privacy protections – especially with the changes to data residency. Is this true?**

- Most other jurisdictions in Canada have been operating safely for years without similar data residency restrictions.
- Our proposed framework builds on and improves what the other provinces have.
- Data residency doesn't protect information; effective controls protect information.

**Key Messages / Topic Scripts / Questions and Answers**  
**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**  
**October 21, 2021**

---

- Even Europe's General Data Protection Regulation – widely lauded as the world's most robust privacy law – doesn't restrict data residency.
  - No other province mandates privacy management programs like we are proposing.
  - The level of protection should reflect the level of risk involved, which is why we are strengthening due diligence requirements for public bodies, particularly requiring privacy impact assessments.
  - Often, because of the Act's current data-residency requirements, public bodies are forced to use services that are perhaps less secure than similar services offered by more established tech companies based abroad.
  - These larger companies, based abroad, have more resources devoted to data security, with some large tech firms investing over \$1 billion per year to keep information secure.
  - In cases where there has been a breach of personal information that could cause significant harm, we will require public bodies to notify the affected person and the Office of the Information and Privacy Commissioner.
- 6. The privacy commissioner, privacy groups and others believe that relaxing data-residency requirements is a step backward. What do you say to those concerned about the perceived softening of privacy protections?**
- Updated data residency requirements will bring B.C. in line with the rest of Canada, who have been managing information safely without similar restrictions.
  - It's important to remember that data residency doesn't protect information – effective controls protect information.
  - B.C.'s legislation has not kept pace with advancements in technology, or the way people access government services.
  - The pandemic has taught us there is high demand for safe and convenient online services that address the changing needs of people, families and organizations in B.C.
  - It will also increase access to modern tools and technologies, such as cloud-based services, so the public sector can quickly and efficiently respond to people's changing needs.
- 7. You say you care about people's right to privacy and information protection. You've also said for years that B.C.'s data is safe within the borders of Canada – so why are you putting it at risk by allowing it to be stored across borders?**
- We've heard from organizations like universities, health authorities and tech companies that our data residency rules were outdated and stopped them from being competitive or responsive to people's evolving needs.
  - It's our role as your government to listen to what's going on in people's lives and adapt – that's why we're proposing these amendments, and not waiting.
  - People want access to healthcare, education opportunities and the technology that is making their lives easier through COVID.



## Key Messages / Topic Scripts / Questions and Answers

### Freedom of Information and Protection of Privacy Act (FOIPPA) amendments

October 21, 2021

- Today, people can safely and securely access telehealth from home, talk to their doctor via Zoom, learn online, meet with their coworkers and do business, faster.
- The Act's current data-residency requirements are blanket protections that require all personal information to be stored and accessed within Canada, except under limited circumstances, even if the personal information has little-to-no risk of causing harm.
- The level of protection should reflect the level of risk involved, which is why we are strengthening due diligence requirements for public bodies, particularly requiring privacy impact assessments.
- Privacy impact assessments consider risk on a case-by-case basis, based on the expected activities and sensitivity of the information involved.
- Often, because of the Act's current data-residency requirements, public bodies are forced to use services that are perhaps less secure than similar services offered by more established tech companies based abroad.
- These larger companies, based abroad, have more resources devoted to data security, with some large tech firms investing over \$1 billion per year to keep information secure.
- Most data are encrypted in multiple layers, regardless of where it is stored.

#### **8. Will these amendments put health information at risk? With HLTH GCPE for approval**

- This FOIPPA change will align data residency requirements, creating consistency across the health sector and providing opportunities to store data with greater security.
- Now, healthcare providers will be able to access to more specialized diagnostic testing tools outside the country.
- Patients will also have access to more tools to help them manage their healthcare with better security to keep their data safe.
- People can safely and securely access telehealth from home or talk to their doctor via Zoom: services that are making people's lives easier through COVID.
- None of that was possible under the old legislation, and the order making these advancements possible expires at the end of this year.
- We learned from the pandemic that we can safely make these changes.
- It's important to remember that your information is safe, no matter where it is stored and that it's protected by many layers of protection and encryption.
- Data residency doesn't protect information – effective privacy controls protect information.
- And because of the Act's current data-residency requirements, often public bodies are forced to use services that are possibly less secure than those offered by established tech companies based abroad.
- The amendments don't change government's need for Canadian datacentres. Where our service providers have Canadian options, we will opt for those.
- The Patriot Act in the US does not pose the same risks it did when data residency was first added to the Act. Technology evolution, new protections and legislation replacing the Patriot Act have all resulted in much less risk.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- The Act already requires ministries to conduct a Privacy Impact Assessment (PIA), which considers risk, case by case, based on the specific activities and information involved and with our changes all public bodies will be required to conduct a PIA when disclosing sensitive information.
  - Often, because of the Act's current data-residency requirements, public bodies are forced to use services that are possibly less secure than similar services offered by established tech companies based abroad that may have more resources to devote to data security.
  - We spend approximately \$25 million each year on information security, but the large tech firms spend over \$1 billion per year – each.
- 9. The pandemic may have shown us better ways to do things, but it also opened us up to increased and more sophisticated cyber threats. How are you keeping our information safe from cyber criminals?**
- In this age of increased cyber security risk, people are understandably concerned about their privacy and protecting their personal information. So are we.
  - Privacy breaches can happen in any jurisdiction, whether the data is stored in a filing cabinet, in a computer system or on a cloud.
  - We are making these changes based on the advice of privacy experts and are confident in the multiple layers of encryption and security measures in place to protect people's data.
- 10. Many of the applications that will use, or store peoples' information are cloud-based. We've seen prominent people have their cloud-based information compromised. How are you going to protect our cloud-based information?**
- Larger, more established tech companies abroad have more resources devoted to data security, with some large tech firms investing over \$1 billion per year to keep information secure.
  - Data is encrypted through multiple layers of protection, regardless of where it is stored.
  - Notably, cloud computing is already used to house non-critical data belonging to:
    - The U.S. Department of Defence
    - National Bank of Canada
    - Interpol
  - In cases where there has been a breach of personal information that could cause significant harm to someone, we will require public bodies to notify the affected person and the Office of the Information and Privacy Commissioner.
  - This will ensure people understand how their information has been handled and allow them to make choices for their own protection.
  - We are strengthening that privacy impact assessments (PIAs) are required by all public bodies, which will ensure that public servants are conducting the due diligence necessary to appropriately handle personal information.

**Key Messages / Topic Scripts / Questions and Answers**  
**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**  
**October 21, 2021**

---

**11. What about the risks posed by the U.S. Patriot Act? British Columbians' information could be compromised by American authorities and we wouldn't be able to stop it.**

- Data residency is not the only way to protect information.
- Strong technical controls can be effective in keeping data out of the hands of others.
- When American law enforcement needs B.C. data, there are legal government-to-government processes that can be used.
- The Patriot Act in the US does not pose the same risks it did when data residency was first added to the Act.
- Technology evolution, new protections and legislation replacing the Patriot Act have all resulted in less risk. Broad requests and bulk data collection are no longer permitted.
- The USA Freedom and Cloud acts, which replace much of the Patriot Act, also include a process for challenging requests that did not exist under the Patriot Act.
- Increased automation further decreases risk because it reduces the number of people that can see information and includes new security measures that better protect information.
- This means that it is more difficult to make legitimate law enforcement requests for B.C. data when appropriate controls are in place.

**12. The privacy commissioner says he wasn't consulted on the changes to data-residency requirements. Why wouldn't you consult the commissioner on something so important?**

- The proposed amendments have been informed through regular meetings and consultation with the Office of the Information and Privacy Commissioner (OIPC), including 18 engagements between April and September 2021.
- While we regularly consult the OIPC on privacy-related issues, their duty isn't to set policy.
- We heard from several public bodies that data residency requirements were making them less competitive and making it harder to deliver the services people deserve.
- The pandemic has taught us that there is a high demand for safe, convenient online services and that we need to remain flexible to keep pace with advancements in technology and the way people access government services.
- We must balance the advice of the OIPC and our top priority of information privacy with our duty to provide responsive, modern services to people in B.C.
- Our amendments have been informed by comprehensive consultation and feedback from the public, Indigenous partners, businesses and organizations.

**13. When was section 13 of FOIPPA introduced?**

- Section 13 [Policy advice or recommendations] has remained relatively unchanged since the Act first came into force in 1993.
- Minor amendments to this section were last made in 2011, but these were unrelated to issues raised by the Commissioner.

**Key Messages / Topic Scripts / Questions and Answers**  
**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**  
**October 21, 2021**

---

**14. Both the Commissioner and the Special Committee have recommended amending s13. Why aren't you doing this?**

- The 2015/16 Special Committee report identified concerns about the scope of S.13.
- Specifically, the Special Committee recommended establishing a publication scheme that would apply to all public bodies for mandatory proactive disclosure of those records listed in s. 13(2)(a) to (n)
- While all recommendations made by the OIPC and past Special Committees were thoroughly reviewed, this is not under consideration at this time.
- Government would like to ensure that the ability for public servants to have full and frank discussion of policy issues remains intact.

**15. How does the application of Section 13 of FOIPPA to “factual information” compare against other jurisdictions?**

- The laws governing freedom of information in Ontario and Newfoundland contain very similar language to FOIPPA on this issue.
- Most other jurisdictions across Canada take a narrower approach to background information that is used for policy development. A common approach in other provinces is that the head of a public body cannot consider “background research of a scientific or technical nature” as advice or recommendations.
- Some others, such as Quebec, and the federal government, do not clearly address the issue of background information used in policy development.

**16. Have there been any significant court rulings respecting the interpretation of section 13 that have implications for B.C.?**

- On May 9, 2014, the Supreme Court of Canada (SCC) ruled on an appeal of an Ontario court decision involving an FOI request where Ontario's Ministry of Finance denied the applicant access to the records on the basis that they would reveal advice or recommendations of a public servant (similar to s. 13 of B.C.'s FOIPPA).
- An Adjudicator in the Office of the Information and Privacy Commissioner of Ontario ordered the disclosure of the records and denied the Ministry's application for reconsideration.
- While the Superior Court later dismissed the Ministry's subsequent application for judicial review, the Court of Appeal found the disclosure order was unreasonable, allowed the appeal and remitted the matter to the Ontario IPC.
- The SCC found that the terms "advice" and "recommendations" have distinct meaning and held that "advice" was broader than "recommendations".
- The SCC decision supported and aligns with the B.C. government's interpretation of FOIPPA s. 13.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- The SCC's reasoning focused on maintaining the confidentiality needed to ensure an effective public service; the protection of advice and recommendations is vital to ensuring free and frank discussions within the public service.

**17. What happens if we don't make this change to data residency requirements?**

- People have come to depend on the use of a variety of tools that have been available to them through the pandemic.
- The ministerial order allowing these tools by law will expire at the end of the year.
- The current restrictions force public bodies to use less effective and sometimes less secure technology solutions. Our vendors are moving to international solutions and are leaving B.C. behind without any alternatives.
- This means that, without change, public bodies in B.C. may be forced to build their own systems, at great expense, because they won't be able to access solutions on the market that comply with B.C.'s strict data-residency rules.
- Lack of access to modern tools and technologies also poses a risk to public bodies' innovation and competitiveness. For example, greater access to cloud-based services will improve B.C. post-secondary institutions' ability to attract students by allowing them to use many of the cloud-based education tools that their competitors can offer outside of B.C.

**18. What privacy protection controls are you putting in place to reinforce the province's role in safeguarding information given the relaxation of data-residency requirements?**

- The existing government requirements for a privacy management program to be in place will be extended to the entire public sector. A privacy management program includes governance, accountability, policies, processes and training on protecting information.
- Context is critical - privacy protection controls should be scaled to the potential risks to information and based on the specific context of that information.
- These changes will also allow the use of security tools that were not previously available to B.C. public bodies – for example, tools that help scan emails for different threats.
- In cases where there has been a breach of personal information that could cause significant harm to someone, we will be requiring public bodies to notify the affected person and the Office of the Information and Privacy Commissioner.
- This will ensure people understand how their information has been handled and allow them to make choices for their own protection.
- We are requiring all public bodies to conduct privacy impact assessments (PIAs), to ensure they appropriately handle personal information.
- And it's important to remember that storing personal data outside of Canada is not new: there are 30 existing purposes under the Act currently that permit this.

**19. What is mandatory breach reporting and why is it just now being introduced?**

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- Mandatory breach reporting is current practice in provincial ministries and requires public bodies to notify affected individuals and the privacy commissioner in the event of a privacy breach where there is reasonable expectation of significant harm.
- We are strengthening government accountability and transparency by making this current policy and best practice mandatory for both ministries and the broader public sector.

**20. Why is mandatory breach reporting coming into force later?**

- We intend to bring mandatory breach reporting into force one year after Royal Assent to give public bodies time to prepare for new legal requirements.
- Government will continue this practice, as it has been doing for many years.

**CONSULTATION:**

**21. I thought you consulted with public institutions about fees and that they advocated for them? But some are saying they didn't advocate for fees?**

- I'd like to clarify my previous comments about the FOIPPA consultation with public bodies.
- We consulted with thousands of people, businesses, Indigenous communities and public sector bodies, including health authorities and post-secondary institutions.
- As part of our extensive consultation process, we brought recommendations to participants and asked for their feedback on how an application fee may or may not impact their organization.
- I can confirm that public bodies didn't advocate for fees during consultation.
- We also did not hear any objections.
- We took the feedback we received into consideration as we drafted proposed amendments and thank the thousands of people who helped us.

**22. How have you consulted people prior to making these amendments?**

- We have heard from thousands of people, Indigenous communities businesses and organizations.
- The proposed amendments reflect what we've heard through many engagements and consultations including with Indigenous communities, the public, input from subject-matter experts across government, and recommendations from the OIPC and past Special Committees of the Legislative Assembly.
- In 2018-19, substantial engagement was completed to identify stakeholder concerns and priority issues including through an online govTogetherBC public engagement, a series of roundtables with key stakeholder groups, discussions with Indigenous communities and a mail-out campaign asking for input and recommendations from over 200 First Nations communities.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- Building on these earlier consultations, between April and August 2021, the Ministry of Citizens' Services re-engaged with many of the same groups, including government ministries, broader public sector public bodies, municipalities, Indigenous leaders and communities, the B.C. tech sector, the OIPC and the general public to confirm previous inputs and gain a current understanding of potential impacts.
- Feedback was received through Minister and ADM roundtable meetings, presentations to stakeholder groups, meetings with ministry staff, two public surveys administered by govTogetherBC and Ipsos, which received 1,600 and 800 responses, respectively, a questionnaire distributed to leaders in the over 200 First Nations in B.C., and discussions with Treaty First Nations representatives.

**23. Which Indigenous partners have you spoken with?**

- The Ministry of Citizens' Services has had meaningful discussions with the Union of BC Indian Chiefs, First Nations Summit, First Nations Leadership Council, the BC Assembly of First Nations.
- The Ministry also engaged with Treaty First Nations including meetings with representatives from the five Maa-nulth nations, Tsawwassen First Nation and the Nisga'a Lisims Government.
- To gain the perspective of Indigenous Peoples on access to information and privacy, we have twice invited leaders of over 200 B.C. First Nations to provide input, most recently, through an online questionnaire.
  - In response to this invitation, representatives from the Stk'emlupsemc Te Secwepemc Nation requested a meeting with Ministry staff, which was held in early September 2021.
- In alignment with B.C.'s Declaration Act, we will continue to work in consultation and co-operation with Indigenous Peoples as we move forward with this work.

**24. Did you consult with advocacy groups such as the B.C. Freedom of Information and Privacy Association (FIPA)? If yes, how did you consider their input?**

- We engaged with FIPA in 2018-19 on similar amendments.
- We also considered FIPA's submissions to previous Special Committees of the Legislative Assembly that reviewed the Act when developing our amendments package.
- In summer 2021, we focused on talking to directly impacted stakeholders and partners, such as public bodies, the OIPC, the public and Indigenous representatives.

**25. How will the amendments address previous Special Committee and Commissioner recommendations?**

- Recommendations by privacy experts, including the OIPC and Special Committee, are integral to our proposed amendments.

**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- There are many longstanding recommendations from previous Special Committees of the Legislative Assembly that reviewed the Act, and from the Information and Privacy Commissioner.
- The proposed amendments address several of these recommendations, including recommendations about mandatory breach reporting, privacy management programs and subsidiary corporations.
- Several of their other recommendations have also been addressed through policy, for example, FOI applicant anonymity protection.
- And we have issued several new proactive disclosure directives in recent years to address recommendations related to government accountability and transparency.

**26. Why aren't you waiting for the new Special Committee's recommendations?**

- The ministerial order that currently allows government to offer services that people have come to expect in the digital era is expiring at the end of December.
- For example, right here in the house with Zoom...
- The last two Special Committees made several recommendations that were not enacted by the previous government.
- In fact, the Act has not been substantially updated since 2011.
- The legislation tabled this week includes many of the recommendations of the past two Special Committees, such as:
  - Making the destruction of documents to evade access an offense; and
  - Making it mandatory to notify individuals and the commissioner of privacy breaches.
- We've also acted on other key recommendations to create a duty to document and expand proactive disclosures.
- We anticipate that the new Special Committee would, if we waited to amend the Act, repeat many of these previous recommendations.
- Updating the Act now allows the new Special Committee to focus on emerging issues.
- This legislation allows us to continue offering these services to people in BC while the Special Committee does its important work.

**FEES**

**27. How will a fee help deliver better services to people, and get them the information they are entitled to under the very Act you are amending?**

- You only have to take a look at other jurisdictions to see how implementing a modest fee helps reduce overall FOI requests.
- Right now, B.C. receives more FOI requests annually than the three western provinces, combined.
- The fee was designed so people can access the information they need, but currently can't because a small group of requestors are overloading the system.



**Key Messages / Topic Scripts / Questions and Answers**

**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**

**October 21, 2021**

---

- It's slowing down our ability to get people's personal information to them, and that's unacceptable.
- If charging a modest fee for non-personal requests helps people focus their request, then we know we're on the right track.

**28. If your government is all about making life more affordable, why are you adding yet another fee?**

- We're proposing a modest fee that will only impact those making general, non-personal requests.
- Those asking for personal information will continue to not pay a fee at all.
- This isn't about revenue, this is about supporting the people making information requests to focus them so they get the most useful information, faster.

**29. The fee seems like a money grab. Is the deficit so big that you need to nickel and dime people?**

- A modest application fee is about reinforcing the spirit and intent of the Act.
- Those requesting their own personal information will continue to pay no fee at all.
- Under the old legislation, people waited too long for the information they deserve because of a small number of requestors whose broad and often vexatious requests for information were slowing down the system.
- Government processes more than 10,000 freedom of information requests each year and the average cost of processing a single FOI request is \$3,000, though some large, complex requests can exceed this.
- The volume of requests has increased by more than 40% over a two-year period, reaching an all-time high of over 13,000 requests in 2019/20 (13,055).
- Adding a fee to non-personal FOI requests is in line with other jurisdictions in Canada. It wasn't a barrier to information elsewhere and it won't be here in B.C.
- The fee will apply to only those requesting non-personal requests – **mostly** to the top 2% of frequent requestors. The application fee is not intended to recover the cost – or even a significant portion of the costs – for an information request.
- The intent is to encourage applicants to be more specific in their requests about the records they are seeking, and the ministries they are seeking the records from, so that we can improve freedom of information services for people so they can get their information, faster.

**30. The fee seems targeted at media and political parties. Are you trying to stifle requests? What are you hiding?**

- Those making personal requests will continue to pay no fee at all.

**Key Messages / Topic Scripts / Questions and Answers**  
**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**  
**October 21, 2021**

---

- By making the fee for non-personal requests modest, we are ensuring the application fee is not a barrier to information access.
- People, businesses and organizations deserve to have timely access to information.
- They do not get full value from the FOI system when it is inundated by a small number of applicants making overly broad or intentionally vexatious requests.
- The fee is intended to focus requests made and improve B.C.'s freedom of information services to the thousands of people who request access to information every year.

**31. You haven't been explicit on how much this 'application fee' will be. How much are you planning to charge people for public access to information?**

- B.C.'s modest fee will not be a barrier to access and it won't apply to those requesting their own information.
- Across Canada, application fees for general information requests range from \$5 to \$50. B.C.'s will be consistent with other administrative fees.
- Other provinces have been charging fees for more than a decade.
- The fee will be set through regulation following Royal Assent.

**32. How much revenue is the application fee expected to raise and where will it go?**

- We expect approximately \$100,000 annually will be generated by application fees.
- This is a fraction of more than an estimated \$30 million annually that it costs to process general FOI requests.

[NOT for sharing: proposing it go into CIRMO streams; need TBS approval before sharing]

**33. What happens if a request is met with a no records response? Do people get their money back?**

- This is a modest application fee, not a response fee.
- Requestors are encouraged to be as focused and specific as possible in their request in order to get the information that they are seeking.
- There will be no refunds.

**34. Are there other jurisdictions that charge a fee for information access?**

- The federal government, Alberta, Ontario, PEI and Nova Scotia and Nunavut charge application fees for general access to information requests.
- In Saskatchewan, local governments charge for their access to information requests.
- Fees in other jurisdictions range from \$5 - \$50.

**Key Messages / Topic Scripts / Questions and Answers**  
**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**  
**October 21, 2021**

---

**35. So who are making the most requests? Can you prove that a small portion of applicants are backing up the system?**

- The two most prolific FOI applicants in 2020-21 were:
  - One political party requestor with 4,772 requests at a cost of \$14.3 million. That's more than 13 requests a day.
  - And one media requestor with 397 requests at a cost of \$1.2 million. That's more than one a day, for every day of the year.
- By comparison, all other media requestors combined accounted for 328 requests at a cost of \$1 million.
- If applicants were encouraged to focus their requests, it would save the FOI system from having to seek and produce sometimes upwards of thousands of records that aren't helpful to the applicant but are extremely time and resource-consuming to produce.
- If we can make changes to help people get the information they deserve, faster, we're going to do it.

**36. So, the application fee is about putting a stop to one political party's and one media outlet's perceived, excessive requests?**

- As in other jurisdictions, the modest fee is meant to encourage requestors to focus on the information that they need and deserve, not thousands of pages that are of no use to the applicant.
- If we can help people get the information they need, faster, by introducing a modest fee, then we will.
- People do not get full value from the FOI system when it is inundated by a small number of applicants.
- The backlog created by a handful of high-volume requestors has a direct impact on the resources available to respond to others – such as personal requests from youth in care, inmates, and disability or income assistance requestors.
- The application fee is intended to reinforce the spirit and intent of the Act by encouraging applicants to be more focused when making requests, which will free up resources so that we can be more responsive to requests that we receive.

**37. Health Authorities are saying they didn't advocate for the FOI fees – is that accurate?**

- A proposed FOI application fee is to focus the significant volume of FOI requests and ensure that public resources are also focused on giving people access to the information as quickly and easily as possible.
- Consultation engagements were held with public bodies in June 2021, including post-secondary institutions and health authorities, to hear broad feedback on FOIPPA.
- The organizations were presented with an overview of the broad amendments including FOI potential changes.

**Key Messages / Topic Scripts / Questions and Answers**  
**Freedom of Information and Protection of Privacy Act (FOIPPA) amendments**  
**October 21, 2021**

---

- Feedback from both post-secondary and health authorities were focused on data residency, with the health authorities also speaking to the substantial increase of general requests during the COVID-19 pandemic. Feedback included encouragement to review the fees as they currently don't align with the cost of processing a request.
- Public sector comments focussed on operational impacts related to FOI requests, the results of both the govTogetherBC and Ipsos surveys highlighted that the accuracy of the information the public receives from government through the FOI processes is paramount. The speed of response and low/no fees were secondary.

**38. It sometimes takes several attempts to get an FOI right – that's going to get very expensive. How are you ensuring people don't get dinged unjustly?**

- B.C. is committed to providing timely and helpful FOI service to the people of British Columbia.
- Applying an application fee will help preserve FOI resources for people who use the system to access the information they need, including citizens requesting access to their own personal information.
- FOI staff regularly work with applicants to assist in focussing their requests so that they can receive the information they need, faster and more efficiently.
- FOI staff will be available to support requestors in identifying which ministry may hold the records they are seeking.

**OTHER:**

**39. How was this legislation reviewed using a GBA+ lens?**

- For one, we're removing all gendered and non-inclusive language from the legislation.
- The legislation hasn't been substantially updated since 2011; we had a lot of work to do.

**40. When will the amendments come into force?**

- All amendments to the Act are anticipated to come into force within a year.
- Some amendments won't come into force immediately so that public bodies can prepare to meet the new legal requirements.