Re: Certificate of readiness - Approval needed

From: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To: Scott, Samantha CITZ:EX
Cc: Lawal, Kassandra CITZ:EX
Sent: October 5, 2021 2:46:34 PM PDT

Approved

Honourable Lisa Beare, Minister
Ministry of Citizens' Services
250-356-8247



On Oct 5, 2021, at 2:43 PM, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca> wrote:

Hi Minister,
This is the final version of your FOIPPA bill, all minor changes in response to comments made in LRC. Below is the list of changes made since you last sign the certificate of readiness.
s.13

Following the LRC meeting on the 21st, the Ministry of Citizens' Services received correspondence from Chief Justice Robert Bauman, Chief Justice Christopher Hinkson and Chief Judge Melissa Gillespie who were provided with a consultation draft of the Bill in early September. s.13
s.13 s.14
s.14

s.14 Due to unforeseen drafting delays, these edits could not be completed prior to the LRC meeting on the 21st.
Please let me know if you approve and we will add you esig.
Thankyou
Samantha Scott | Ministerial Advisor to the Honourable Minister Beare
Ministry of Citizens' Services
PO Box 9044 Stn Prov Gov, Victoria, BC, V8W 9E2 | 778-679-4889
<1 - FIPPA_DRAFT BILL C45 draft 17 - Oct 1 2021.docx>
<1A - FIPPA Certificate of Readiness.docx>
<BN to LRC Chair - Changes made to Bill - Freedom of Information and Protection of Privacy Amendment Act.docx>

RE: Final Prep Session Before Intro of Bill (Part 2) - October 14th Update

From: Leppard, Brianna CITZ:EX <Brianna.Leppard@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 12, 2021 12:04:10 PM PDT

Absolutely, thanks Kass!
Brianna

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 12, 2021 11:39 AM
To: Leppard, Brianna CITZ:EX <Brianna.Leppard@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Subject: RE: Final Prep Session Before Intro of Bill (Part 2) - October 14th Update
Perhaps let's keep that 15 minutes and use that time for Marie to do a final round-up with MLB after staff sign off.
Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Leppard, Brianna CITZ:EX <Brianna.Leppard@gov.bc.ca>
Sent: October 12, 2021 10:44 AM
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Subject: Final Prep Session Before Intro of Bill (Part 2) - October 14th Update
Hi both,
As per Jennifer's request, we have been asked to shorten the "Final Prep Session Before Intro of Bill (Part 2)" meeting on October 14th by 15 minutes, to occur from 2:00-2:45 pm instead. CJ and the DM are attending the DMC Committee meeting together and will be presenting during their meeting. I have updated the Minister's calendar and will let Marie know.
Thank you so much,
Brianna Leppard | Administrative Coordinator
Honourable Lisa Beare's Office | Minister of Citizens' Services
Phone: 250-883-4368

Update FOIPPA Material (eApp 17840)

From:	Cook, Jeannette CITZ:EX <Jeannette.Cook@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent:	October 13, 2021 4:54:47 PM PDT
Attachments:	12 - Summary of OIPC concerns - Oct 12 2021_FINAL for Binder CLEAN.docx, 6 - Appendix to House and Section Notes - v1,0.docx, 9 - FOIPPA - Qs and As - Full - Oct 12 2021.docx, 3 - SN Second Reading Notes_FOIPPA amendments_UPDATED (gcpe edits) CLEAN.docx, 4 - Committee Stage Beginning Notes.doc, 12 - Summary of OIPC concerns - Oct 12 2021_FINAL for Binder TRACKED.docx, 11 - Key facts and figures_October 2021.docx, 10 - 3 Column Document - For Back Pocket.docx, 3 - SN Second Reading Notes_FOIPPA amendments_UPDATED (gcpe edits) TRACKED.docx, 5 - House and Section Notes Oct 12 FINAL.docx, 1 - Proposed Content-Bill.docx, 2 - SN First Reading Notes_FOIPPA amendments_UPDATED (gcpe edits).docx, 7 - SN Third Reading Notes_FOIPPA amendments.docx, 1A - FIPPA Certificate of Readiness (final signed).pdf

Hi Kass,

Attached is the updated FOIPPA package for the prep meeting tomorrow. eApp coming your way right now as well.

The track changes version are here for the two docs:

Have a lovely night.

JC

Jeannette Cook| Director, Executive Operations
Deputy Minister's Office | Ministry of Citizens' Services
Ph: 250 387-8817 | e: jeannette.cook@gov.bc.ca

Page 004 of 513 to/à Page 006 of 513

Withheld pursuant to/removed as

s.12 ; s.13

Page 007 of 513 to/à Page 012 of 513

Withheld pursuant to/removed as

s.13

FOR REVIEW -- FW: Updated FOIPPA Material (eApp 17840)

From:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To:	Beare, Lisa CITZ:EX
Sent:	October 13, 2021 5:01:24 PM PDT
Attachments:	4 - Committee Stage Beginning Notes.doc, 6 - Appendix to House and Section Notes - v1,0.docx, 1 - Proposed Content-Bill.docx, 9 - FOIPPA - Qs and As - Full - Oct 12 2021.docx, 12 - Summary of OIPC concerns - Oct 12 2021_FINAL for Binder CLEAN.docx, KMQA FOIPPA amendments - 13Oct2021 - Draft11.docx, 10 - 3 Column Document - For Back Pocket.docx, 11 - Key facts and figures_October 2021.docx, 7 - SN Third Reading Notes_FOIPPA amendments.docx, 3 - SN Second Reading Notes_FOIPPA amendments_UPDATED (gcpe edits) CLEAN.docx, 1A - FIPPA Certificate of Readiness (final signed).pdf, 2 - SN First Reading Notes_FOIPPA amendments_UPDATED (gcpe edits).docx, 5 - House and Section Notes Oct 12 FINAL.docx

Hi Minister

Updated FOIPPA materials from DMO below, as well as and updated KMQA with key question scripts from Kirsten – for prep session tomorrow, 2-3pm. Staff will attend until 2:45 and then you have wrap up time with Marie. We are also scheduling a short check-in with Marie for Monday.

Cheers,
Kass

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

BEGINNING OF COMMITTEE STAGE

Second reading is finished and the Bill is on the Order Paper under Committee

- The House leader calls, “Committee stage debate on Bill XX *2021*”
- The Speaker calls the Chairman of the Committee and vacates the chair.
- The Chairman of the Committee takes the Chair, calls the whole Committee to order and proceeds with consideration of the bill, **section by section** **(See TAB 5)**
- Members may speak more than once on each section and amendment.
- The Chariman calls the question on each section, amendment and title.

DRAFT

Appendix: Repealed and Replaced Sections in the *Freedom of Information and Protection of Privacy Act* (FOIPPA)

Scope of the Act

3 (1) This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:

(a) a court record, a record of a judge of the Court of Appeal, Supreme Court or Provincial Court, a record of a master of the Supreme Court, a record of a justice of the peace, a judicial administration record or a record relating to support services provided to the judges of those courts;

(b) a personal note, communication or draft decision of a person who is acting in a judicial or quasi judicial capacity;

(c) subject to subsection (3), a record that is created by or for, or is in the custody or control of, an officer of the Legislature and that relates to the exercise of that officer's functions under an Act;

(c.1) [Repealed 2002-50-19.]

(c.2) subject to subsection (4), a record that is created by or for, or is in the custody or control of, the auditor general appointed under the *Auditor General for Local Government Act* and that relates to the exercise of his or her functions under that Act;

(d) a record of a question that is to be used on an examination or test;

(e) a record containing teaching materials or research information of

(i) a faculty member, as defined in the *College and Institute Act* and the *University Act*, of a post-secondary educational body,

(ii) a teaching assistant or research assistant employed at a post-secondary educational body, or

(iii) other persons teaching or carrying out research at a post-secondary educational body;

(f) material placed in the digital archives or the museum archives of government by or for a person or agency other than a public body;

(g) material placed in the archives of a public body by or for a person or agency other than a public body;

(h) a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed;

(i) [Repealed 2011-17-1.]

(j) a record that is available for purchase by the public;

(k) a record of a service provider that is not related to the provision of services for a public body.

(2) This Act does not limit the information available by law to a party to a proceeding.

(3) The following sections apply to officers of the Legislature, their employees and, in relation to their service providers, the employees and associates of those service providers, as if the officers and their offices were public bodies:

(a) section 30 [*protection of personal information*];

(b) section 30.1 [*storage and access must be in Canada*];

(c) section 30.2 [*obligation to report foreign demand for disclosure*];

(d) section 30.3 [*whistle-blower protection*];

(e) section 30.4 [*unauthorized disclosure prohibited*];

(e.1) section 30.5 [*notification of unauthorized disclosure*];

(f) section 33 [*disclosure of personal information*];

(g) section 33.1 [*disclosure inside or outside Canada*];

(h) section 33.2 [*disclosure inside Canada only*];

(i) section 74.1 [*privacy protection offences*].

(4) The sections referred to in subsection (3) apply to the auditor general appointed under the *Auditor General for Local Government Act*, employees appointed under that Act and, in relation to service providers to the auditor general, the employees and associates of those service providers, as if the auditor general and his or her office were public bodies.

Obligation to report foreign demand for disclosure

30.2 (1) In this section:

"**foreign demand for disclosure**" means a subpoena, warrant, order, demand or request that is

(a) from a foreign court, an agency of a foreign state or another authority outside Canada, and

(b) for the unauthorized disclosure of personal information to which this Act applies;

"**unauthorized disclosure of personal information**" means disclosure of, production of or the provision of access to personal information to which this Act applies, if that disclosure, production or access is not authorized by this Act.

(2) If the head of a public body or an employee, officer or director of a public body or an employee or associate of a service provider

(a) receives a foreign demand for disclosure,

(b) receives a request to disclose, produce or provide access to personal information to which this Act applies, if the public body, employee or other person receiving the request

(i) knows that the request is for the purpose of responding to a foreign demand for disclosure, or

(ii) has reason to suspect that it is for such a purpose, or

(c) has reason to suspect that unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure,

the head of the public body, the employee or other person must immediately notify the minister responsible for this Act.

(3) The notice under subsection (2) must include, as known or suspected,

(a) the nature of the foreign demand for disclosure,

(b) who made the foreign demand for disclosure,

(c) when the foreign demand for disclosure was received, and

(d) what information was sought by or disclosed in response to the foreign demand for disclosure.

Disclosure of personal information

33 A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3.

Disclosure inside or outside Canada

33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

(a) in accordance with Part 2;

(a.1) if the information or disclosure is of a type described in section 22 (4) (e), (f), (h), (i) or (j);

(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;

(c) in accordance with an enactment of British Columbia, other than this Act, or Canada that authorizes or requires its disclosure;

(c.1) if it is made available to the public in British Columbia under an enactment, other than this Act, that authorizes or requires the information to be made public;

(d) in accordance with a provision of a treaty, arrangement or written agreement that

(i) authorizes or requires its disclosure, and

(ii) is made under an enactment of British Columbia, other than this Act, or Canada;

(e) to an individual who is a minister, an officer of the public body or an employee of the public body other than a service provider, if

(i) the information is necessary for the performance of the duties of the minister, officer or employee, and

(ii) in relation to disclosure outside Canada, the outside disclosure is necessary because the individual is temporarily travelling outside Canada;

(e.1) to an individual who is a service provider of the public body, or an employee or associate of such a service provider, if

(i) the information is necessary for the performance of the duties of the individual in relation to the public body, and

(ii) in relation to disclosure outside Canada,

(A) the individual normally receives such disclosure only inside Canada for the purpose of performing those duties, and

(B) the outside disclosure is necessary because the individual is temporarily travelling outside Canada;

(f) to an officer or employee of the public body or to a minister, if the information is immediately necessary for the protection of the health or safety of the officer, employee or minister;

(g) to the Attorney General or legal counsel for the public body, for the purpose of preparing or obtaining legal advice for the government or public body or for use in civil proceedings involving the government or public body;

(h) to the minister responsible for the *Coroners Act* or a person referred to in section 31 (1) of that Act, for the purposes of that Act;

(i) if

(i) the disclosure is for the purposes of collecting amounts owing to the government of British Columbia or a public body by

(A) an individual, or

(B) a corporation of which the individual the information is about is or was a director or officer, and

(ii) in relation to disclosure outside Canada, there are reasonable grounds for believing that

(A) the individual the information is about is in, resides in or has assets in the other jurisdiction, or

(B) if applicable, the corporation was incorporated in, is doing business in or has assets in the other jurisdiction;

(i.1) for the purposes of

(i) a payment to be made to or by the government of British Columbia or a public body,

(ii) authorizing, administering, processing, verifying or canceling such a payment, or

(iii) resolving an issue regarding such a payment;

(j) [Repealed 2011-17-13.]

(k) for the purposes of

(i) licensing or registration of motor vehicles or drivers, or

(ii) verification of motor vehicle insurance, motor vehicle registration or drivers licences;

(l) for the purposes of licensing, registration, insurance, investigation or discipline of persons regulated inside or outside Canada by governing bodies of professions and occupations;

(m) if

(i) the head of the public body determines that compelling circumstances exist that affect anyone's health or safety, and

(ii) notice of disclosure is mailed to the last known address of the individual the information is about, unless the head of the public body considers that giving this notice could harm someone's health or safety;

(m.1) for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur;

(n) so that the next of kin or a friend of an injured, ill or deceased individual may be contacted;

(o) in accordance with section 36 [*disclosure for archival or historical purposes*];

(p) if the disclosure

(i) is necessary for

(A) installing, implementing, maintaining, repairing, trouble-shooting or upgrading an electronic system or equipment that includes an electronic system, or

(B) data recovery that is being undertaken following the failure of an electronic system

that is used in Canada, by the public body or by a service provider for the purposes of providing services to a public body, and

(ii) in the case of disclosure outside Canada, results in temporary access and storage that is limited to the minimum period of time necessary to complete the installation, implementation, maintenance, repair, trouble-shooting, upgrading or data recovery referred to in subparagraph (i);

(p.1) if the disclosure

(i) is necessary for the processing of information and if that processing does not

(A) involve the intentional access of the information by an individual, or

(B) result in the storage of personal information, other than personal information that is metadata, outside Canada, and

(ii) in the case of disclosure outside Canada, results in temporary access that is limited to the minimum period of time necessary to complete the processing;

(p.2) if the information is metadata that

(i) is generated by an electronic system, and

(ii) describes an individual's interaction with the electronic system,

and if,

(iii) if practicable, personal information in individually identifiable form has been removed from the metadata or destroyed, and

(iv) in the case of disclosure to a service provider, the public body has prohibited any subsequent use or disclosure of personal information in individually identifiable form without the express authorization of the public body;

(q) if the information was collected by observation at a presentation, ceremony, performance, sports meet or similar event

(i) at which the individual voluntarily appeared, and

(ii) that was open to the public;

(r) if the information

(i) was disclosed on a social media site by the individual the information is about,

(ii) was obtained or compiled by the public body for the purpose of enabling the public body to engage individuals in public discussion or promotion respecting proposed or existing initiatives, policies, proposals, programs or activities of the public body or respecting legislation relating to the public body, and

(iii) is disclosed for a use that is consistent with the purpose described in subparagraph (ii);

(s) in accordance with section 35 [*disclosure for research or statistical purposes*];

(t) to comply with a subpoena, a warrant or an order issued or made by a court, person or body in Canada with jurisdiction to compel the production of information.

(2) In addition to the authority under any other provision of this section or section 33.2, a public body that is a law enforcement agency may disclose personal information referred to in section 33

(a) to another law enforcement agency in Canada, or

(b) to a law enforcement agency in a foreign country under an arrangement, a written agreement, a treaty or provincial or Canadian legislative authority.

(3) The minister responsible for this Act may, by order, allow disclosure outside Canada under a provision of section 33.2 in specific cases or specified circumstances, subject to any restrictions or conditions that the minister considers advisable.

(4) In addition to the authority under any other provision of this section or section 33.2, the Insurance Corporation of British Columbia may disclose personal information if

(a) the information was obtained or compiled by that public body for the purposes of insurance provided by the public body, and

(b) disclosure of the information is necessary to investigate, manage or settle a specific insurance claim.

(5) In addition to the authority under any other provision of this section or section 33.2, a provincial identity information services provider may disclose personal identity information

(a) to enable the provincial identity services provider to provide services under section 69.2, or

(b) to a public body if the disclosure is necessary to enable the public body to identify an individual for the purpose of providing a service to the individual.

(6) In addition to the authority under any other provision of this section or section 33.2, a public body may disclose personal identity information to a provincial identity information services provider if the disclosure is necessary to enable

(a) the public body to identify an individual for the purpose of providing a service to the individual, or

(b) the provincial identity information services provider to provide services under section 69.2.

(7) Without limiting the authority under any other provision of this section or section 33.2, a public body may disclose personal information to the individual the information is about if

(a) the individual has initiated contact with the public body about a matter and the public body is responding to that contact,

(b) the public body discloses information only in respect of the matter, and

(c) the public body uses

(i) the same communication method used by the individual to initiate contact, or

(ii) another communication method authorized by the individual.

Disclosure inside Canada only

33.2 A public body may disclose personal information referred to in section 33 inside Canada as follows:

(a) for the purpose for which it was obtained or compiled or for a use consistent with that purpose (see section 34);

(b) [Repealed 2011-17-14.]

(c) to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister;

(d) to an officer or employee of

(i) a public body, or

(ii) an agency,

or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties, respecting the common or integrated program or activity, of the officer, employee or minister to whom the information is disclosed;

(e) to an officer or employee of a public body or to a minister, if the information is necessary for the protection of the health or safety of the officer, employee or minister;

(f) to the auditor general or any other prescribed person or body for audit purposes;

(g) to a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem;

(h) to a representative of the bargaining agent, who has been authorized in writing by the employee whom the information is about, to make an inquiry;

(i) to a public body or a law enforcement agency in Canada to assist in a specific investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result;

(j) to the digital archives, the museum archives of government or the archives of a public body, for archival purposes;

(k) [Repealed 2011-17-14.]

(l) to an officer or employee of a public body or to a minister, if the information is necessary for the purposes of planning or evaluating a program or activity of a public body.

Disclosure for research or statistical purposes

35 (1) A public body may disclose personal information in its custody or under its control for a research purpose, including statistical research, only if

(a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form or the research purpose has been approved by the commissioner,

(a.1) subject to subsection (2), the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in the research,

(b) any data linking is not harmful to the individuals that information is about and the benefits to be derived from the data linking are clearly in the public interest,

(c) the head of the public body concerned has approved conditions relating to the following:

(i) security and confidentiality;

(ii) the removal or destruction of individual identifiers at the earliest reasonable time;

(iii) the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of that public body, and

(d) the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public body's policies and procedures relating to the confidentiality of personal information.

(2) Subsection (1) (a.1) does not apply in respect of research in relation to health issues if the commissioner approves

(a) the research purpose,

(b) the use of disclosed information for the purpose of contacting a person to participate in the research, and

(c) the manner in which contact is to be made, including the information to be made available to persons contacted.

Disclosure for archival or historical purposes

36 (1) In addition to the authority under sections 33.1, 33.2 and 33.3, the digital archives, the museum archives of government or the archives of a public body may disclose personal information in its custody or under its control for archival or historical purposes if

(a) the disclosure would not be an unreasonable invasion of personal privacy under section 22,

(b) the disclosure is for historical research and is in accordance with section 35,

(c) the information is about someone who has been dead for 20 or more years, or

(d) the information is in a record that has been in existence for 100 or more years.

(2) For the purposes of subsection (3), "institution" means a museum, an archives or a similar institution that is or forms part of a public body or an organization, as the latter is defined in the *Personal Information Protection Act*.

(3) A board or a francophone education authority, as those are defined in the *School Act*, may disclose personal information in its custody or under its control to an institution if

(a) the disclosure would not be an unreasonable invasion of personal privacy under section 22,

(b) the disclosure is for historical research and is in accordance with section 35,

(c) the information is about someone who has been dead for 20 or more years, or

(d) the information is in a record that has been in existence for 100 or more years.

Data-linking initiatives

36.1 (1) A public body participating in a new or significantly revised data-linking initiative must comply with the regulations, if any, prescribed for the purposes of this subsection.

(2) If all the participants in a new or significantly revised data-linking initiative are a health care body, the ministry of the minister responsible for the administration of the *Ministry of Health Act* or a health-related organization as prescribed, then subsection (1) does not apply to the participants.

(3) For the purposes of subsections (1) and (2), a public body is participating in

(a) a new data-linking initiative if the data-linking initiative is implemented after the date this section comes into force, or

(b) a significantly revised data-linking initiative if the data-linking initiative is an existing data-linking initiative and a public body participating in that data-linking initiative expands it by doing one or more of the following:

(i) adding a public body or an agency that is not already a participant in the data-linking initiative;

(ii) adding a database that is not already a part of the data-linking initiative;

(iii) undertaking a purpose that is not already a purpose of the data-linking initiative;

(iv) using a type of technology that is not already a part of the data-linking initiative.

(4) Despite subsection (3) (a), a public body is not participating in a new data-linking initiative if, before the date this section comes into force, the public body has completed a written project plan respecting the data-linking initiative that states

(a) the objectives of the project,

(b) the costs and benefits of the project, and

(c) the risks associated with those costs and benefits.

General offences and penalties

74 (1) A person must not wilfully do any of the following:

(a) make a false statement to, or mislead or attempt to mislead, the commissioner or another person in the performance of the duties, powers or functions of the commissioner or other person under this Act;

(b) obstruct the commissioner or another person in the performance of the duties, powers or functions of the commissioner or other person under this Act;

(c) fail to comply with an order made by the commissioner under section 54.1 or 58 or by an adjudicator under section 65 (2).

(2) A person who contravenes subsection (1) commits an offence and is liable to a fine of up to $5 000.

(3) Section 5 of the *Offence Act* does not apply to this Act

Privacy protection offences

74.1 (1) A person who contravenes section 30.4 [*unauthorized disclosure*] or 30.5 [*notification of unauthorized disclosure*] commits an offence.

(2) A person who is a service provider or an employee or associate of a service provider commits an offence if the person does any of the following:

(a) stores or allows access to personal information to which section 30.1 [*location and access in Canada*] applies contrary to that section;

(b) contravenes section 30.2 [*obligation to report foreign demand for disclosure*];

(c) contravenes section 30.3 [*whistle-blower protection*].

(3) If an employee or associate of a service provider

(a) stores or allows access to personal information to which section 30.1 applies contrary to that section,

(b) contravenes section 30.2,

(c) contravenes section 30.3,

(d) contravenes section 30.4, or

(e) contravenes section 30.5,

in relation to personal information that is held because of the service provider's status as a service provider, the service provider commits an offence.

(4) If a corporation commits an offence under this section, an officer, director or agent of the corporation who authorizes, permits or acquiesces in the commission of the offence also commits an offence, whether or not the corporation is prosecuted for the offence.

(5) A person who commits an offence under this section is liable

(a) in the case of an individual, other than an individual who is a service provider, to a fine of up to $2 000,

(b) in the case of a partnership that is or individual who is a service provider, to a fine of up to $25 000, and

(c) in the case of a corporation, to a fine of up to $500 000.

(6) The time limit for laying an information to commence a prosecution for an offence under this section is

(a) one year after the date on which the act or omission that is alleged to constitute the offence occurred, **or**

(b) if the minister responsible for this Act issues a certificate described in subsection (7), one year after the date on which the minister learned of the act or omission referred to in paragraph (a).

(7) A certificate purporting to have been issued by the minister responsible for this Act certifying the date referred to in subsection (6) (b) is proof of that date.

(8) In a prosecution for an offence under this section, it is a defence for the person charged to prove that the person exercised due diligence to avoid the commission of the offence.

Fees

75 (1) The head of a public body may require an applicant who makes a request under section 5 to pay to the public body fees for the following services:

(a) locating, retrieving and producing the record;

(b) preparing the record for disclosure;

(c) shipping and handling the record;

(d) providing a copy of the record.

(2) An applicant must not be required under subsection (1) to pay a fee for

(a) the first 3 hours spent locating and retrieving a record, or

(b) time spent severing information from a record.

(3) Subsection (1) does not apply to a request for the applicant's own personal information.

(4) If an applicant is required to pay a fee for services under subsection (1), the head of the public body

(a) must give the applicant a written estimate of the total fee before providing the service, and

(b) may require the applicant to pay a deposit in the amount set by the head of the public body.

(5) If the head of a public body receives an applicant's written request to be excused from paying all or part of the fees for services, the head may excuse the applicant if, in the head's opinion,

(a) the applicant cannot afford the payment or for any other reason it is fair to excuse payment, or

(b) the record relates to a matter of public interest, including the environment or public health or safety.

(5.1) The head of a public body must respond under subsection (5) in writing and within 20 days after receiving the request.

(6) The fees that prescribed categories of applicants are required to pay for services under subsection (1) may differ from the fees other applicants are required to pay for them, but may not be greater than the actual costs of the services.

Page 030 of 513 to/à Page 059 of 513

Withheld pursuant to/removed as

s.12 ; s.13 ; s.14

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

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. If data residency provisions are repealed, how will sensitive personal information be protected? 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 *Declaration on the Rights of Indigenous Peoples Act* (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 *Hospital (Auxiliary) Act*....51
Q1. Why is the removal of the reference to the *Hospital (Auxiliary) Act* 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 52
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.

s.13

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.
- The proposal to introduce an application fee for access requests is not expected to be a significant revenue source. In fact, the average FOI request costs government $3,000 to process, and the application fee will, s.13 be modest in comparison.

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 s.14 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 suppling 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

s.13

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. s.13

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 s.14 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.Maximum Offence Penalties.

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

ts

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. 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 113 of 513 to/à Page 115 of 513

Withheld pursuant to/removed as

s.12 ; s.13

Page 116 of 513 to/à Page 131 of 513

Withheld pursuant to/removed as

s.13

Page 132 of 513 to/à Page 139 of 513

Withheld pursuant to/removed as

s.12 ; s.13

FOIPPA facts and figures

There are more than 2,900 public bodies covered by the Freedom of Information and Protection of Privacy Act including government ministries, Crown corporations, and local public bodies such as municipalities, universities, colleges, school boards and health authorities.

BC Government FOIPPA by the numbers (2020/21)

10,265	Total number of FOI requests (6,467 general and 3,798 personal)
$30 million	Total annual cost for government to process general FOI requests
$51,000	Total fees collected by Ministries for FOI requests
3.3 million	Number of responsive pages processed
85%	On time response rate for FOI requests
58	Average number of days to process an FOI request
$3,000	Average cost to government to process one FOI request
62%	Percent of the general requests from political parties
3,521	Proactive disclosures made under Ministerial directives
90%	Percentage of ministry employees completed privacy/FOI training
972	Number of privacy impact assessments conducted

FOI requests

- One political party requestor has made 4,772 requests at a cost of $14.3 million – that's more than 13 requests a day.
    - This requester makes more general requests in a year than the province of Alberta receives from all general requesters in a year.
- One media requestor with 397 requests at a cost of $1.2 million – that's more than one per day.
- All other media requestors combined accounted for 328 requests at a cost of $1 million.
- Approximately 98% of applicants make fewer than five requests annually, with most making only one.
- B.C. receives requests per capita than in the three prairie provinces (AB, SK, MB) combined.
- Under the existing fee schedule (which allows fees to be charged for locating/producing records), the average amount recouped per FOI request is $5. Fees are only collected in 2% of all general requests.

Fees

Jurisdiction	**Application Fee**
Alberta	$25 for first request / $50 per continuing request
Saskatchewan	$20 per requests to local governments
Ontario	$5 per request
Nova Scotia	$5 per request
Prince Edward Island	$5 per request
Nunavut	$25 per request
Canada	$5 per request

Manitoba, Quebec, New Brunswick, Newfoundland and Labrador, Yukon and Northwest Territories have no fees.

Privacy

Data residency restrictions

- Provisions in Privacy Legislation
    - Nova Scotia has specific provisions related to data residency outlined in their legislation.
    - Quebec describes the parameters required for disclosure outside Quebec (public body responsibility to ensure equivalent protection or else it must refuse to release)
    - Some other jurisdictions have some data residency requirements in sector specific legislation (e.g. Health sector), or in policy.

Privacy management programs

- With these amendments BC will be the only jurisdiction in Canada to require privacy management programs in law.

Information security spending

- BC government spends approximately $25 million each year on information security whereas many large tech firms can each spend over $1 billion per year.

FOIPPA consultations (April to September 2021)

1,600 and 800	Responses to two public surveys
200+	Leaders of First Nations in B.C. surveyed (12 total responses across 2 separate surveys)
60+	Organizations participated in roundtable conversations
100+	Engagements with B.C broader public sector bodies, government ministries, Indigenous partners, the technology sector, the Office of the Information and Privacy Commissioner and the public
18	Engagements with the Office of the Information and Privacy Commissioner

Special Committees of the Legislative Assembly

- While all recommendations made by the 2010/11 and 2015/16 Special Committees have been thoroughly reviewed, not all of the recommendations will be addressed through this package.
    - 9 recommendations will be addressed through the Bill.
    - 8 recommendations have been addressed either through policy or other means.
    - 22 recommendations remain unaddressed.
- Proposals to address Special Committee recommendations 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.

Appendix: Detailed data

Types of FOI requests	2018/19	2019/20	2020/21
General	7,622	8,147	6,467
Personal	4,633	4,908	3,798
Total	12,255	13,055	10,265*

* drop in volume is attributed to significantly fewer requests from political parties and individuals during the COVID-19 pandemic.

General FOI requests by applicant type	2019/20	2020/21
Political Party	5,836	4,033
Individual	946	896
Media	536	760
Business	302	238
Law Firm	213	214
Interest Group	195	210
Researcher	68	87
Other Government	34	17
Other Public Body	17	12

FOIs	2019/20	2020/21
Total Number of FOI Requests Closed	12,899	10,841
Total Number of General Requests Closed	8,317	7,151
Number of Requests Where Fees Paid	145	144
Sum of Fees Paid (nearest thousand)	$44,000	$51,000
Percent of General Requests Where Fees Paid	1.74%	2.01%
Average Fee per FOI Request	$3	$5

PIAs	2019/20	2020/21
Total PIA	1,171	972
Operational PIA	846	620
LPIA/RPIA	325	352

Privacy	2019/20	2020/21
Reported (Privacy Breaches and Complaints)	2,234	1,977
Investigations Conducted	1,889	1,622
Violations Occurred	1,405	1,493

Proactive disclosure	2018/19	2019/20	2020/21
FOI requests	2,493	2,570	1,841
Other directives	1,533	1,494	1,680
Total	4,026	4,064	3,521

THIRD READING SPEAKING NOTES
(FOLLOWING COMMITTEE)

Bill XX – 2021

Freedom of Information and Protection of Privacy Amendment Act 2021

When the title has passed,

OPTION 1 - WITHOUT AMENDMENT

Minister: "I move that the Committee rise and report the Bill complete without amendment."

[Committee Chair: Puts motion, Chair sends for the Speaker and when the Speaker has taken the Chair:

The Committee Chair: "The Committee on **Bill No. XX** reports the Bill complete without amendment."

The Speaker asks: "When shall the Bill be read a third time?"]

Minister: "Now, Mister Speaker."

[Speaker: "The question is Third Reading of **Bill No. XX**
Speaker announces result of vote and
if the "ayes" have it, declares the Bill "an act".]

OR

DRAFT

OPTION 2 - WITH AMENDMENT

Minister: **"Mister Speaker, I move that the Committee rise and report Bill XX complete with amendments."**

[Committee Chair: Puts motion, Chair sends for the Speaker and when the Speaker has taken the Chair:

The Committee Chair: "The Committee on Bill No**. XX** reports the Bill complete with amendment."

The Speaker asks: "When shall the Bill be considered as reported?"]

Minister: **"With leave of the House, now, Mister Speaker."**

OR

"At the next sitting, Mister Speaker."

DRAFT

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

Page 146 of 513 to/à Page 148 of 513

Withheld pursuant to/removed as

s.13

s.13

Closing

s.13

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:

5

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 151 of 513

Withheld pursuant to/removed as

s.12 ; s.13 ; s.14

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.]

Freedom of Information and Protection of Privacy Act Amendments

House and Section Notes

Section 1 ***of the Freedom of Information and Protection of Privacy Amendment Act, 2021***

amends subsection 2 (1) (c) of the
Freedom of Information and Protection of Privacy Act

Purpose of this Act

2 (1) The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by

(a) giving the public a right of access to records,

(b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,

(c) specifying limited exceptions to the ~~rights~~ right of access,

(d) preventing the unauthorized collection, use or disclosure of personal information by public bodies, and

(e) providing for an independent review of decisions made under this Act.

Page 157 of 513

Withheld pursuant to/removed as

s.13

Section 2 of the *Freedom of Information and Protection of Privacy Amendment Act*, 2021

repeals section 3 of the
Freedom of Information and Protection of Privacy Act and **substitutes**
a new subsection 3 (1)

~~**Scope of this Act**~~

~~**3** (1) Subject to This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:~~

[see Appendix for full section repealed]

Application

3 (1) Subject to subsections (3) to (5), this Act applies to all records in the custody or under the control of a public body, including court administration records.

Page 159 of 513

Withheld pursuant to/removed as

s.13

Section 2 of the *Freedom of Information and Protection of Privacy Amendment Act*, 2021

repeals section 3 of the
Freedom of Information and Protection of Privacy Act and **substitutes**
a new subsection 3 (2)

3 (2) Part 3 applies

(a) to all employees, officers and directors of a public body, and

(b) in the case of an employee that is a service provider, to all employees and associates of the service provider.

Page 161 of 513

Withheld pursuant to/removed as

s.13

Section 2 of the *Freedom of Information and Protection of Privacy Amendment Act*, 2021

repeals section 3 of the
Freedom of Information and Protection of Privacy Act and **substitutes**
a new subsection 3 (3)

3 (3) This Act does not apply to the following:

(a) a court record;

(b) a record of

(i) a judge of the Court of Appeal, Supreme Court or Provincial Court,

(ii) a master of the Supreme Court, or

(iii) a justice of the peace;

(c) a judicial administration record;

(d) a record relating to support services provided to a judge of a court referred to in paragraph (b) (i);

(e) a personal note, communication or draft decision of a person who is acting in a judicial or quasi-judicial capacity;

(f) a record that is created by or for, or is in the custody or under the control of, an officer of the Legislature and that relates to the exercise of functions under an Act;

(g) a record that is created by or for, or is in the custody or under the control of

the auditor general under the *Auditor General for Local Government Act* and that relates to the exercise of functions under that Act;

(h) a record of a question or **answer** to be used on an examination or test;

(i) a record containing teaching or research materials of

i) a faculty member, as defined in the *College and Institute Act* and the *University Act*, of a post-secondary educational body,

(ii) a teaching assistant or research assistant employed at a post-secondary educational body, or

(iii) another person teaching or carrying out research at a post-secondary educational body;

(j) a record placed in the archives of a public body, or the digital archives or museum archives of government, by or for a person or agency other than a public body;

(k) a record relating to a prosecution if not all proceedings in respect of the prosecution have been completed;

(l) a record of a service provider that is not related to the provision of services for a public body.

Page 163 of 513

Withheld pursuant to/removed as

s.13

Section 2 of the *Freedom of Information and Protection of Privacy Amendment Act*, 2021

repeals section 3 of the
Freedom of Information and Protection of Privacy Act and **substitutes**
a new subsection 3 (4)

3 (4) This Act, other than sections 30, 30.3, 30.5 (2), 33 and 65.3 to 65.6, does not apply to

(a) an officer of the Legislature, including all employees of the officer of the Legislature and, in the case of an employee that is a service provider, all employees and associates of the service provider, or

(b) the auditor general under the *Auditor General for Local Government Act*, including all employees of that auditor general and, in the case of an employee that is a service provider, all employees and associates of the service provider.

Page 165 of 513

Withheld pursuant to/removed as

s.13

Section 2 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals section 3 of the
Freedom of Information and Protection of Privacy Act and **adds**
a new subsection 3 (5)

3 (5) Part 2 does not apply to the following:

(a) a record that is available for purchase by the public;

(b) a record that does not relate to the business of the public body;

(c) a record of metadata that

(i) is generated by an electronic system, and

(ii) describes an individual's interaction with the electronic system;

(d) an electronic record that has been lawfully deleted by an employee of a public body and can no longer be accessed by the employee.

Page 167 of 513

Withheld pursuant to/removed as

s.13

Section 2 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals section 3 of the
Freedom of Information and Protection of Privacy Act and **adds**
a new subsection 3 (6)

3 (6) This Act does not limit the information available by law to a party to a proceeding.

Page 169 of 513

Withheld pursuant to/removed as

s.13

Section 2 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals section 3 of the
Freedom of Information and Protection of Privacy Act and **adds**
a new subsection 3 (7)

3 (7) If a provision of this Act is inconsistent or in conflict with a provision of another Act, this Act prevails unless the other Act expressly provides that it, or a provision of it, applies despite this Act.

Page 171 of 513

Withheld pursuant to/removed as

s.13

Section 2 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces section 4 of the *Freedom of Information and Protection of Privacy Act* **to amend the provisions respecting access rights**

Information rights

~~**4** (1) A person who makes a request under section 5 has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.~~
~~(2) The right of access to a record does not extend to information excepted from disclosure under Division 2 of this Part, but if that information can reasonably be severed from a record an applicant has the right of access to the remainder of the record.~~
~~(3) The right of access to a record is subject to the payment of any fee required under section 75.~~

4 (1) Subject to subsections (2) and (3) an applicant who makes a request under section 5 has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.

(2) The right of access to a record does not extend to information that is excepted from disclosure under Division 2 of this Part, but if that information can reasonably be severed from a record, an applicant has a right of access to the remainder of the record.

(3) The right of access to a record is subject to the payment of fees, if any, required under section 75.

Page 173 of 513

Withheld pursuant to/removed as

s.13

Section 3 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 5 (1) (a) of the
Freedom of Information and Protection of Privacy Act

How to make a request

5 (1) To obtain access to a record, the applicant must make a written request that

(a) provides ~~sufficient~~ enough detail to enable an experienced employee of the public body, with a reasonable effort, to identify the ~~records sought~~ record sought,

(b) provides written proof of the authority of the applicant to make the request, if the applicant is acting on behalf of another person in accordance with the regulations, and

(c) is submitted to the public body that the applicant believes has custody or control of the record.

Page 175 of 513

Withheld pursuant to/removed as

s.13

Section 4 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 6 (2) of the
Freedom of Information and Protection of Privacy Act

Duty to assist applicants

6 (1) The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.

(2) Moreover, the head of a public body ~~must create a record for an applicant~~ must create for an applicant a record to which section 4 gives a right of access

(a) the record can be created from a machine readable record in the custody or under the control of the public body using its normal computer hardware and software and technical expertise, and

(b) creating the record would not unreasonably interfere with the operations of the public body.

Page 177 of 513

Withheld pursuant to/removed as

s.13

Section 5 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 7 of the
Freedom of Information and Protection of Privacy Act

Time limit for responding

~~**7** (4) If the head of a public body determines that an applicant is to pay fees for services related to a request, the 30 days referred to in subsection (1) do not include the period from the start of the day the head of the public body gives the applicant a written estimate of the total fees to the end of the day one of the following occurs:~~

~~(a) the head of the public body excuses the applicant from paying all of the fees under section 75 (5) ;~~

~~(b) the head of the public body excuses the applicant from paying part of the fees under section 75 (5), and the applicant agrees to pay the remainder and, if required by the head of a public body, pays the deposit required;~~

~~(c) the applicant agrees to pay the fees set out in the written estimate and, if required by the head of a public body, pays the deposit required.~~

7 (4) If the head of a public body determines that an applicant is to pay fees under section 75 (1) (a) or (b), the 30 days referred to in subsection (1) of this section do not include the period of time from that determination until one of the following occurs:

(a) the head of the public body excuses the applicant from paying all of the fees for services;

(b) the head of the public body excuses the applicant from paying some of the fees for services and the applicant agrees to pay the remainder and, if required by the head of the public body, pays the deposit required;

(c) the applicant agrees to pay the fees for services set out in the written estimate and, if required by the head of the public body, pays the deposit required;

(d) the applicant pays the application fee.

(5) If an applicant asks the commissioner under section 52 (1) to review a fee estimate or a refusal to excuse the payment of all or part of ~~the fee~~ a fee required by the head of the public body, the 30 days referred to in subsection (1) do not include the period from the start of the day the applicant asks for the review to the end of the day the commissioner makes a decision.

Page 179 of 513

Withheld pursuant to/removed as

s.13

Section 6 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces subsection 8 (1) (c) (ii) of the
Freedom of Information and Protection of Privacy Act

Contents of response

8 (1) In a response under section 7, the head of the public body must tell the applicant

(a) whether or not the applicant is entitled to access to the record or to part of the record,

(b) if the applicant is entitled to access, where, when and how access will be given, and

(c) if access to the record or to part of the record is refused,

(i) the reasons for the refusal and the provision of this Act on which the refusal is based,

(ii) ~~the name, title, business address and business telephone number of an officer or employee of the public body who can answer the applicant's questions about the refusal, and~~

(ii) the contact information of an officer or employee of the public body who can answer the applicant's questions about the refusal, and

(iii) that the applicant may ask for a review under section 53 or 63.

Page 181 of 513

Withheld pursuant to/removed as

s.13

Section 7 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 9 (1) of the
Freedom of Information and Protection of Privacy Act

How access will be given

9 (1) If an applicant is told under section 8 (1) that access will be given, the head of the public body ~~concerned~~ must comply with subsection (2), (2.1) or (3) of this section.

Page 183 of 513

Withheld pursuant to/removed as

s.13

Section 8 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 16 (1) and repeals and replaces subsection 16 (3) of the *Freedom of Information and Protection of Privacy Act*

Disclosure harmful to intergovernmental relations or negotiations

16 (1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

(a) harm the conduct by the government of British Columbia of relations between that government and any of the following or their agencies:

(i) the government of Canada or a province of Canada;

(ii) the council of a municipality or the board of a regional district;

(iii) an ~~aboriginal government~~ indigenous governing entity;

(iv) the government of a foreign state;

(v) an international organization of states,

(b) reveal information received in confidence from a government, council or organization listed in paragraph (a) or their agencies, or

(c) harm the conduct of negotiations relating to ~~aboriginal self-government~~ Indigenous self-government or treaties.

(2) Moreover, the head of a public body must not disclose information referred to in subsection(1) without the consent of

(a) the Attorney General, for law enforcement information, or

(b) the Executive Council, for any other type of information.

~~(3) Subsection(1) does not apply to information that is in a record that has been in existence for 15 or more years unless the information is law enforcement information~~.

(3) Subsection (1) does not apply to information that is in a record that has been in existence for 15 or more years unless the information is

(a) law enforcement information, or

(b) information referred to in subsection (1) (a) (iii) or (c)

Page 185 of 513

Withheld pursuant to/removed as

s.13

Section 9 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

adds section 18.1 to the
Freedom of Information and Protection of Privacy Act

Disclosure harmful to interests of an Indigenous people

18.1 (1) The head of a public body must refuse to disclose information if the disclosure could reasonably be expected to harm the rights of an Indigenous people to maintain, control, protect or develop any of the following with respect to the Indigenous people:

(a) cultural heritage;

(b) traditional knowledge;

(c) traditional cultural expressions;

(d) manifestations of sciences, technologies or cultures

(2) Subsection (1) does not apply if the Indigenous people has consented in writing to the disclosure.

Page 187 of 513

Withheld pursuant to/removed as

s.13

Section 10 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 21 (3) (b) of the
Freedom of Information and Protection of Privacy Act

Disclosure harmful to the business interests of a third party

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

(a) the third party consents to the disclosure, or

(b) the information is in a record that is ~~in the custody or control of the archives of the government of British Columbia or~~ in the custody or under the control of the digital archives or museum archives of government or the archives of a public body and that has been in existence for 50 or more years.

Page 189 of 513

Withheld pursuant to/removed as

s.13

Section 11 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 22 of the
Freedom of Information and Protection of Privacy Act

Disclosure harmful to personal privacy

22 (2) In determining under subsection (1) or (3) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether [….]

(d) the disclosure will assist in researching or validating the claims, disputes or grievances of ~~aboriginal people~~ Indigenous peoples, […]

(3) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if [….]

~~h) the disclosure could reasonably be expected to reveal the content of a personal recommendation or evaluation, a character reference or a personnel evaluation supplied by the third party in confidence and the applicant could reasonably be expected to know the identity of the third party~~,

h) the disclosure would reveal

(i) the identity of a third party who supplied, in confidence, a personal recommendation or evaluation, character reference or personnel evaluation, or

(ii) the content of a personal recommendation or evaluation, character reference or personnel evaluation supplied, in confidence, by a third party, if the applicant could reasonably be expected to know the identity of the third party,

(4) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if [ ]

(d) the disclosure is for a research or statistical purpose and is in accordance with ~~section 35~~ section 33 (4),

Page 191 of 513

Withheld pursuant to/removed as

s.13

Section 12 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section subsections 23 (1) and (2) of the
Freedom of Information and Protection of Privacy Act

Notifying the third party

23 (1) If the head of a public body intends to give access to a record that the head has reason to believe contains information that might be excepted from disclosure under ~~section 21 or 22~~ section 18.1, 21 or 22, the head must give the third party a written notice under subsection (3).

(2) If the head of a public body does not intend to give access to a record that contains information excepted from disclosure under ~~section 21 or 22~~ section 18.1, 21 or 22, the head may give the third party a written notice under subsection (3).

Page 193 of 513

Withheld pursuant to/removed as

s.13

Section 13 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

adds section 25.1 to Division 1 of Part 3 of the
Freedom of Information and Protection of Privacy Act

Unauthorized collection, use and disclosure of personal information prohibited

25.1 An employee, officer or director of a public body or an employee or associate of a service provider must not collect, use or disclose personal information except as authorized by this Act.

Page 195 of 513

Withheld pursuant to/removed as

s.13

Section 14 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 27 (1) of the
Freedom of Information and Protection of Privacy Act

How personal information is to be collected

27 (1) A public body must collect personal information directly from the individual the information is about unless […]

(b) the information may be disclosed to the public body under sections ~~33 to 36~~ section 33, ~~to 36~~

(c) the information is collected for the purpose of

(i) determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary,

(ii) a proceeding before a court or a judicial or ~~quasi judicial~~ quasi-judicial tribunal,

(iii) collecting a debt or fine or making a payment,

(iv) law enforcement, or

(v) reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur,

(c.1) the information is collected from a body disclosing it in accordance with a provision of a treaty, arrangement or written agreement that

(i) authorizes or requires the disclosure, and

(ii) is made under an enactment of British Columbia, other than this Act, or an enactment of Canada,

(c.2) the information is collected from a body disclosing it under an enactment of another province or of Canada,

Page 197 of 513

Withheld pursuant to/removed as

s.13

Section 14 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces subsection 27 (2) (c) of the
Freedom of Information and Protection of Privacy Act

How personal information is to be collected

27 (2) A public body must ensure that an individual from whom it collects personal information is told

(a) the purpose for collecting it,

(b) the legal authority for collecting it, and

~~(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.~~

(c) the contact information of an officer or employee of the public body who can answer the individual's questions about the collection.

Page 199 of 513

Withheld pursuant to/removed as

s.13

Section 15 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces subsection 29 (1) of the
Freedom of Information and Protection of Privacy Act

Right to request correction of personal information

~~**29** (1) An applicant who believes there is an error or omission in his or her personal information may request the head of the public body that has the information in its custody or under its control to correct the information.~~

29 (1) An individual who believes there is an error or omission in personal information about the individual that is in the custody or under the control of a public body may request the head of the public body to correct the information.

Page 201 of 513

Withheld pursuant to/removed as

s.13

Section 16 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 30 of the
Freedom of Information and Protection of Privacy Act

Protection of personal information

30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized ~~access,~~ ~~collection~~ collection~~,~~ use, disclosure, disposal.

Page 203 of 513

Withheld pursuant to/removed as

s.13

Section 17 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 30.1, 30.2, 30.4 and 30.5 (1) of the
Freedom of Information and Protection of Privacy Act

~~**Storage and access must be in Canada**~~

~~**30.1** A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:~~

~~(a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;~~

~~(b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;~~

~~(c) if it was disclosed under section 33.1 (1) (i.1).~~

~~**Obligation to report a foreign demand for disclosure**~~

~~**30.2** (1) In this section:~~

~~"foreign demand for disclosure" means a subpoena, warrant, order, demand or request that is~~

~~(a) from a foreign court, an agency of a foreign state or another authority outside Canada, and~~

~~(b) for the unauthorized disclosure of personal information to which this Act applies~~;

[see Appendix for full repeal]

~~**Unauthorized disclosure prohibited**~~

~~**30.4** An employee, officer or director of a public body or an employee or associate of a service provider who has access, whether authorized or unauthorized, to personal information in the custody or control of a public body, must not disclose that information except as authorized under this Act.~~

Notification of unauthorized disclosure

~~**30.5** (1) In this section, "unauthorized disclosure of personal information" has the same meaning as in section 30.2 (1).~~

(2) An employee, officer or director of a public body, or an employee or associate of a service provider, who knows that there has been an unauthorized disclosure of personal information that is in the custody or under the control of the public body must immediately notify the head of the public body.

Page 205 of 513

Withheld pursuant to/removed as

s.13

Section 18 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 30.3 of the
Freedom of Information and Protection of Privacy Act

Protection of personal information

Whistle-blower protection

30.3 An employer, whether or not a public body, must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee of the employer, or deny that employee a benefit, because

~~(a) the employee, acting in good faith and on the basis of reasonable belief, has notified the minister responsible for this Act under section 30.2,~~

(b) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the commissioner that the employer or any other person has contravened or is about to contravene this Act,

(c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene this Act,

(d) the employee, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention of this Act, or

(e) the employer believes that an employee will do anything described in paragraph ~~(a),~~ (b), (c) or (d).

Page 207 of 513

Withheld pursuant to/removed as

s.13

Section 19 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals section 31.1 of the
Freedom of Information and Protection of Privacy Act

~~**Application to employees and others**~~

~~**31.1** The requirements and restrictions established by this Part also apply to~~
~~(a) the employees, officers and directors of a public body, and~~
~~(b) in the case of an employee that is a service provider, all employees and associates of the service provider~~.

Page 209 of 513

Withheld pursuant to/removed as

s.13

Section 20 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

Repeals and replaces section 32 of the *Freedom of Information and Protection of Privacy Act*

~~**Use of personal information**~~

~~**32** A public body may use personal information in its custody or under its control only~~

~~(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),~~

~~(b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or~~

~~(c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.~~

Use of personal information

32 A public body may use personal information in its custody or under its control only

(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose,

(b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or

(c) for a purpose for which that information may be disclosed to the public body under section 33.

Page 211 of 513

Withheld pursuant to/removed as

s.13

Section 21 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 33, 33.1, 33.2, 35, 36 and substitutes them with new sections 33 and 33.1 of the
Freedom of Information and Protection of Privacy Act

Disclosure of personal information

33 (1) A public body may disclose personal information in its custody or under its control only as permitted by subsections (2) to (9) or by section 33.3.

(2) A public body may disclose personal information in any of the following circumstances:

(a) in accordance with Part 2;

(b) if the information or disclosure is of a type described in section 22 (4) (e), (f), (h), (i) or (j);

(c) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the disclosure;

(d) for the purpose for which the information was obtained or compiled, or for a use consistent with that purpose within the meaning of section 34 *[definition of consistent purpose]*;

(e) in accordance with an enactment of British Columbia or of Canada that authorizes or requires the disclosure;

(f) if the information is made available to the public under an enactment that authorizes or requires the information to be made public;

(g) in accordance with a provision of a treaty, arrangement or written agreement that

(i) authorizes or requires the disclosure, and

(ii) is made under an enactment of British Columbia, other than this Act, or an enactment of Canada;

(h) to an officer or employee of the public body, or to a minister, if the information is necessary for the performance of the duties of the officer, employee or minister;

(i) to an officer or employee of a public body, or to a minister, if the information is necessary to protect the health or safety of the officer, employee or minister;

(j) to an officer or employee of a public body, or to a minister, if the information is necessary for the purposes of planning or evaluating a program or activity of a public body;

Cont'd

Page 213 of 513

Withheld pursuant to/removed as

s.13

Section 21 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 33, 33.1, 33.2, 35, 36 and substitutes them with new sections 33 and 33.1 of the
Freedom of Information and Protection of Privacy Act

Disclosure of personal information (Cont'd)

(k) to an officer or employee of a public body or an agency or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties, respecting the common or integrated program or activity, of the officer, employee or minister to whom the information is disclosed;

(l) to comply with a subpoena, warrant or order issued or made by a court or person in Canada with jurisdiction to compel the production of information in Canada;

(m) to the Attorney General or legal counsel for the public body

(i) for the purpose of preparing or obtaining legal advice for the government or public body, or

(ii) for use in civil proceedings involving the government or public body;

(n) to the minister responsible for the *Coroners Act* or a person referred to in section 31 (1) of that Act, for the purposes of that Act;

(o) for the purpose of collecting amounts owing to the government or a public body by

(i) an individual, or

(ii) a corporation of which the individual the information is about is or was a director or officer;

(p) for the purposes of

(i) a payment to be made to or by the government or a public body,

(ii) authorizing, administering, processing, verifying or cancelling a payment, or

(iii) resolving an issue regarding a payment;

(q) for the purposes of licensing, registering, insuring, investigating or disciplining persons regulated by governing bodies of professions or occupations;

(r) if the information was collected by observation at a presentation, ceremony, performance, sports meet or similar event

(i) that was open to the public, and

(ii) at which the individual the information is about appeared voluntarily;

Cont'd

Page 215 of 513

Withheld pursuant to/removed as

s.13

Section 21 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 33, 33.1, 33.2, 35, 36 and substitutes them with new sections 33 and 33.1 of the
Freedom of Information and Protection of Privacy Act

Disclosure of personal information (Cont'd)

(s) to the auditor general or a prescribed person or body for audit purposes;

(t) if the disclosure is necessary for

(i) installing, implementing, maintaining, repairing, troubleshooting or upgrading an electronic system or equipment that includes an electronic system, or

(ii) data recovery that is undertaken following the failure of an electronic system,

that is used by the public body, or by a service provider for the purposes of providing services to a public body;

(u) if the disclosure is necessary for the processing of information and the following apply:

(i) the processing does not involve the intentional accessing of the information by an individual;

(ii) any processing done outside of Canada is temporary;

(v) if the information is metadata and the following apply:

(i) the metadata is generated by an electronic system;

(ii) the metadata describes an individual's interaction with the electronic system;

(iii) if practicable, information in individually identifiable form has been removed from the metadata or destroyed;

(iv) in the case of disclosure to a service provider, the public body has prohibited subsequent use or disclosure of information in individually identifiable form without the express authorization of the public body;

(w) if the information

(i) was disclosed on social media by the individual the information is about,

(ii) was obtained or compiled by the public body for the purpose of enabling the public body to engage individuals in public discussion or promotion respecting proposed or existing initiatives, policies, programs or activities of the public body or respecting legislation relating to the public body, and

(iii) is disclosed for a use that is consistent with the purpose described in subparagraph (ii);

Page 217 of 513

Withheld pursuant to/removed as

s.13

Section 21 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 33, 33.1, 33.2, 35, 36 and substitutes them with new sections 33 and 33.1 of the
Freedom of Information and Protection of Privacy Act

Disclosure of personal information (Cont'd)

(x) **to an Indigenous governing entity for the purposes of a program or activity that supports the exercise of the rights recognized and affirmed by section 35 of the *Constitution Act*.**

(3) A public body may disclose personal information in any of the following circumstances:

(a) if

(i) the head of the public body determines that compelling circumstances that affect anyone's health or safety exist, and

(ii) notice of disclosure is mailed to the last known address of the individual the information is about, unless the head of the public body considers that the notice could harm anyone's health or safety;

(b) for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur;

(c) to enable the next of kin or a friend of an injured, ill or deceased individual to be contacted;

(d) to a public body, or a law enforcement agency in Canada, to assist in a specific investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result;

(e) to a member of the Legislative Assembly who has been requested by the individual the information is about to assist in resolving a problem;

(f) to a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry;

(g) to the digital archives or museum archives of government or the archives of a public body, for archival purposes;

Cont'd

Page 219 of 513

Withheld pursuant to/removed as

s.13

Section 21 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 33, 33.1, 33.2, 35, 36 and substitutes them with new sections 33 and 33.1 of the
Freedom of Information and Protection of Privacy Act

Disclosure of personal information (Cont'd)

(h) for a research purpose, including statistical research, if

(i) the research purpose cannot be accomplished unless the information is disclosed in individually identifiable form, or the research purpose has been approved by the commissioner,

(ii) the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in the research unless

(A) the research is in relation to health issues, and

(B) the commissioner has approved the research purpose, the use of the information for the purpose of contacting a person to participate in the research and the manner in which contact is to be made, including the information to be made available to the person contacted,

(iii) any data-linking is not harmful to the individual the information is about and the benefits to be derived from the data-linking are clearly in the public interest,

(iv) the head of the public body has approved conditions relating to the following:

(A) security and confidentiality;

(B) the removal or destruction of individual identifiers at the earliest reasonable time;

(C) the prohibition of subsequent use or disclosure of the information in individually identifiable form without the express authorization of the public body, and

(v) the person to whom the information is disclosed has signed an agreement to comply with the approved conditions, this Act and the public body's policies and procedures relating to the confidentiality of personal information.

Leave this page blank

Section 21 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 33, 33.1, 33.2, 35, 36 and substitutes them with new sections 33 and 33.1 of the
Freedom of Information and Protection of Privacy Act

Disclosure of personal information (Cont'd)

33 (4) In addition to the authority under any other provision of this section, the digital archives, museum archives of government or archives of a public body may disclose personal information in its custody or under its control for archival or historical purposes if

(a) the disclosure would not be an unreasonable invasion of personal privacy under section 22,

(b) the information is about an individual who has been deceased for 20 or more years, or

(c) the information is in a record that has been in existence for 100 or more years.

(5) In addition to the authority under any other provision of this section, a board or a francophone education authority, as those are defined in the *School Act*, may disclose personal information in its custody or under its control to a museum, an archives or a similar institution that is or forms part of a public body or an organization, as the latter is defined in the *Personal Information Protection Act*, if

(a) the disclosure would not be an unreasonable invasion of personal privacy under section 22 of this Act,

(b) the information is about an individual who has been deceased for 20 or more years, or

(c) the information is in a record that has been in existence for 100 or more years.

Page 223 of 513

Withheld pursuant to/removed as

s.13

Section 21 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 33, 33.1, 33.2, 35, 36 and substitutes them with new sections 33 and 33.1 of the
Freedom of Information and Protection of Privacy Act

Disclosure of personal information (Cont'd)

33 (6) In addition to the authority under any other provision of this section, a public body that is a law enforcement agency may disclose personal information

(a) to another law enforcement agency in Canada, or

(b) to a law enforcement agency in a foreign state under an arrangement, written agreement or treaty or under provincial or Canadian legislative authority.

(7) In addition to the authority under any other provision of this section, the Insurance Corporation of British Columbia may disclose personal information

(a) for the purposes of

(i) licensing or registering motor vehicles or drivers, or

(ii) verifying motor vehicle registration, insurance or driver licences, or

(b) if

(i) the information was obtained or compiled by the Insurance Corporation of British Columbia for the purposes of insurance it provides, and

(ii) the disclosure is necessary to investigate, manage or settle a specific insurance claim.

(8) In addition to the authority under any other provision of this section, a personal identity information services provider may disclose personal identity information

(a) to enable the personal identity information services provider to provide a service under section 69.2, or

(b) to a public body if the disclosure is necessary to enable the public body to identify an individual for the purpose of providing a service to the individual.

(9) In addition to the authority under any other provision of this section, a public body may disclose personal identity information to a personal identity information services provider if the disclosure is necessary to enable

(a) the public body to identify an individual for the purpose of providing a service to the individual, or

(b) the personal identity information services provider to provide a service under section 69.2.

Page 225 of 513

Withheld pursuant to/removed as

s.13

Section 21 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals sections 33, 33.1, 33.2, 35, 36 and substitutes them with new sections 33 and 33.1 of the
Freedom of Information and Protection of Privacy Act

Disclosure outside of Canada

33.1 A public body may disclose personal information outside of Canada, only if the disclosure is in accordance with the regulations, if any, made by the minister responsible for this Act.

Page 227 of 513

Withheld pursuant to/removed as

s.13

Section 22 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 34 of the
Freedom of Information and Protection of Privacy Act

Definition of consistent purpose

34 For the purposes of ~~section 32 (a), 33.1 (1) (r) (iii) or 33.2 (a), or paragraph (b) of the definition of "data linking" in Schedule 1~~ section 32 (a) or 33 (2) (d) or (w), a use of personal information is consistent with the purpose for which the information was obtained or compiled if the use

(a) has a reasonable and direct connection to that purpose, and

(b) is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.

Page 229 of 513

Withheld pursuant to/removed as

s.13

Section 23 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

Amends the heading for Division 3 of Part 3 of the
Freedom of Information and Protection of Privacy Act

Division 3 — Data-linking ~~Initiatives~~ Programs

Page 231 of 513

Withheld pursuant to/removed as

s.13

Section 24 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces section 36.1 of the
Freedom of Information and Protection of Privacy Act

~~**Data-linking initiatives**~~

~~**36.1** (1) A public body participating in a new or significantly revised data-linking initiative must comply with the regulations, if any, prescribed for the purposes of this subsection.~~

~~(2) If all the participants in a new or significantly revised data-linking initiative are a health care body, the ministry of the minister responsible for the administration of the *Ministry of Health Act* or a health-related organization as prescribed, then subsection(1) does not apply to the participants….~~

[see Appendix for full repeal]

Data-linking programs

36.1 (1) This section does not apply to a data-linking program that is part of research for the purpose of which personal information may be disclosed under section 33 (3) (h).

(2) A public body conducting a data-linking program must comply with the regulations, if any, made for the purposes of this section.

Page 233 of 513

Withheld pursuant to/removed as

s.13

Section 25 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

adds a new Division to Part 3 of the
Freedom of Information and Protection of Privacy Act
entitled:
"Division 4 – Privacy Management Programs and Privacy Breach Notifications"
which includes a new section 36.2 [Privacy management programs]

Privacy management programs

36.2 The head of a public body must develop a privacy management program for the public body and must do so in accordance with the directions of the minister responsible for this Act.

Page 235 of 513

Withheld pursuant to/removed as

s.13

Section 25 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

adds a new Division to Part 3 of the
Freedom of Information and Protection of Privacy Act
entitled:
"Division 4 –Privacy Management Programs and Breach Notifications"
which includes a new section 36.3 [Privacy breach notifications]

Privacy breach notifications

36.3 (1) In this section, **"privacy breach"** means the theft or loss, or the collection, use or disclosure that is not authorized by this Part, of personal information in the custody or under the control of a public body.

(2) Subject to subsection (5), if a privacy breach involving personal information in the custody or under the control of a public body occurs, the head of the public body must, without unreasonable delay,

(a) notify an affected individual if the privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or significant

(i) bodily harm,
(ii) humiliation,
(iii) damage to reputation or relationships,
(iv) loss of employment, business or professional opportunities,
(v) financial loss,
(vi) negative impact on a credit record, or
(vii) damage to, or loss of, property, and

(b) notify the commissioner if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph (a).

(3) The head of a public body is not required to notify an affected individual under subsection (2) if notification could reasonably be expected to

(a) result in immediate and grave harm to the individual's safety or physical or mental health, or
(b) threaten another individual's safety or physical or mental health.

(4) If notified under subsection (2) (b), the commissioner may notify an affected individual.

(5) A notification under subsection (2) (a) or (b) must be made in the prescribed manner.

Page 237 of 513

Withheld pursuant to/removed as

s.13

Section 26 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals subsection 42 (1) (h) of the
Freedom of Information and Protection of Privacy Act

General powers of commissioner

42 (1) In addition to the commissioner's powers and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may

(a) conduct investigations and audits to ensure compliance with any provision of this Act or the regulations,

(b) make an order described in section 58 (3), whether the order results from an investigation or audit under paragraph (a) or an inquiry under section 56,

(c) inform the public about this Act,

(d) receive comments from the public about the administration of this Act,

(e) engage in or commission research into anything affecting the achievement of the purposes of this Act,

(f) comment on the implications for access to information or for protection of privacy of proposed legislative schemes or programs or activities of public bodies,

(g) comment on the implications for access to information or for protection of privacy of automated systems for collection, storage, analysis or transfer of information,

~~(h) comment on the implications for protection of privacy of using or disclosing personal information for data linking,~~

(i) authorize the collection of personal information from sources other than the individual the information is about, and

(j) bring to the attention of the head of a public body any failure to meet the prescribed standards for fulfilling the duty to assist applicants.

Page 239 of 513

Withheld pursuant to/removed as

s.13

Section 27 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces section 43 of the
Freedom of Information and Protection of Privacy Act

~~**Power to authorize a public body to disregard requests**~~

~~**43** If the head of a public body asks, the commissioner may authorize the public body to disregard requests under section 5 or 29 that~~

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

~~(b) are frivolous or vexatious.~~

Power to authorize a public body to disregard a request

43 If the head of a public body asks, the commissioner may authorize the public body to disregard a request under section 5 or 29, including because

(a) the request is frivolous or vexatious,

(b) the request is for a record that has been disclosed to the applicant or that is accessible by the applicant from another source, or

(c) responding to the request would unreasonably interfere with the operations of the public body because the request

(i) is excessively broad, or

(ii) is repetitious or systematic.

Page 241 of 513

Withheld pursuant to/removed as

s.13

Section 28 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 44 (5) of the
Freedom of Information and Protection of Privacy Act

Powers of commissioner in conducting investigations, audits or inquiries

44 (5) After completing a review or investigating a complaint, the commissioner must return any record or any copy of any record ~~produced by the public body concerned~~ produced under subsection (3) by the public body.

Page 243 of 513

Withheld pursuant to/removed as

s.13

Section 29 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 44.1 (1) of the
Freedom of Information and Protection of Privacy Act

Maintenance of order at hearings

44.1 (1) At an oral hearing, the commissioner may make orders or give directions that ~~he or she considers~~ the commissioner considers necessary for the maintenance of order at the hearing, and, if any person disobeys or fails to comply with any order or direction, the commissioner may call on the assistance of any peace officer to enforce the order or direction.

Page 245 of 513

Withheld pursuant to/removed as

s.13

Section 30 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 45 (1) and section 46 of the
Freedom of Information and Protection of Privacy Act

Statements made to the commissioner not admissible in evidence

45 (1) A statement made or an answer given by a person during an ~~investigation or inquiry~~, investigation, audit or inquiry by the commissioner is inadmissible in evidence in court or in any other proceeding, except

(a) in a prosecution for perjury in respect of sworn testimony,

(b) in a prosecution for an offence under this Act, or

(c) in an application for judicial review or an appeal from a decision with respect to that application.

Protection against libel or slander actions

46 Anything said, any information supplied or any record produced by a person during an ~~investigation or inquiry~~ investigation, audit or inquiry by the commissioner is privileged in the same manner as if the ~~investigation or inquiry~~ investigation, audit or inquiry were a proceeding in a court.

Page 247 of 513

Withheld pursuant to/removed as

s.13

Section 31 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 47 (1) of the
Freedom of Information and Protection of Privacy Act

Restrictions on disclosure of information by the commissioner and staff

47 (1) The commissioner and anyone acting for or under the direction of the commissioner must not disclose any information obtained in ~~performing their duties, powers and functions~~ performing their duties or exercising their powers and functions under this Act, except as provided in subsections (2) to (5).

Page 249 of 513

Withheld pursuant to/removed as

s.13

Section 32 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 52 (1) of the
Freedom of Information and Protection of Privacy Act

Right to ask for a review

52 (1) A person who makes a request to the head of a public body, other than the commissioner or the registrar under the *Lobbyists Transparency Act*, for access to a record or for correction of personal information may ask the commissioner to review ~~any decision, act or failure to act~~ any decision, act or failure to act, other than to require an application fee, of the head that relates to that request, including any matter that could be the subject of a complaint under section 42 (2).

Page 251 of 513

Withheld pursuant to/removed as

s.13

Section 33 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 54.1 of the
Freedom of Information and Protection of Privacy Act

Order for severing of records

54.1 (1) After the head of a public body has responded to a request under section 5 and a request for review of that response has been received under section 52, the commissioner may, at any time, by order,

(a) confirm that the ~~head of a public body~~ head of the public body has failed to ~~sever the records~~ sever the information from the records that are the subject of the review, as required by this Act, and

(b) require the head of the public body to ~~sever the records~~ severing information from the records in accordance with the directions and within the period set out in the order

(2) The commissioner may not set a period for ~~severing a record~~ severing information from a record under subsection (1) that is less than 30 days after the date a copy of the order is given to the head of the public body ~~concerned~~.

Page 253 of 513

Withheld pursuant to/removed as

s.13

Section 34 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 60 (2) of the
Freedom of Information and Protection of Privacy Act

Adjudicator to investigate complaints and review decisions

60 (2) An adjudicator may retain the services of any persons necessary to assist the adjudicator in performing ~~his or her functions~~ the adjudicator's functions under this Act.

Page 255 of 513

Withheld pursuant to/removed as

s.13

Section 35 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces section 60.1 of the
Freedom of Information and Protection of Privacy Act

~~**Disregard of request under section 5 or 29**~~

~~**60.1** The commissioner may request an adjudicator designated under section 60 to authorize the commissioner as head of a public body to disregard requests made under section 5 or 29 that~~

~~(a) would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the requests, or~~
~~(b) are frivolous or vexatious~~

Adjudicator may authorize commissioner to disregard requests

60.1 The commissioner may ask an adjudicator designated under section 60 to authorize the commissioner as head of a public body to disregard a request made under section 5 or 29.

Page 257 of 513

Withheld pursuant to/removed as

s.13

Section 36 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 61 (2) of the
Freedom of Information and Protection of Privacy Act

Powers, duties and protections of adjudicator

61 (2) Sections 45, 46, 48 and 50 apply for the purposes of an ~~investigation, inquiry or review~~ investigation, audit or inquiry by an adjudicator.

Page 259 of 513

Withheld pursuant to/removed as

s.13

Section 37 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

adds a new Part 5.1 to the
Freedom of Information and Protection of Privacy Act
entitled "Offences"

PART 5.1 – OFFENCES

Offence Act

65.1 Section 5 of the *Offence Act* does not apply to this Act.

Offence to wilfully mislead, obstruct or fail to comply with commissioner

65.2 A person who wilfully does any of the following commits an offence:

(a) makes a false statement to, or misleads or attempts to mislead,

(i) the commissioner or anyone acting for or under the direction of the commissioner in the performance of duties or exercise of powers and functions under this Act, or

(ii) an adjudicator or anyone acting for or under the direction of an adjudicator in the performance of duties or exercise of powers and functions under this Act;

(b) obstructs

(i) the commissioner or anyone acting for or under the direction of the commissioner in the performance of duties or exercise of powers and functions under this Act, or

(ii) an adjudicator or anyone acting for or under the direction of the adjudicator in the performance of duties or exercise of powers and functions under this Act;

(c) fails to comply with an order made by

(i) the commissioner under section 54.1 or 58, or

(ii) an adjudicator under section 65 (2).

Offence to wilfully evade access provisions

65.3 A person who wilfully conceals, destroys or alters any record to avoid complying with a request for access to the record commits an offence.

Cont'd

Page 261 of 513

Withheld pursuant to/removed as

s.13

Section 37 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

adds a new Part 5.1 to the
Freedom of Information and Protection of Privacy Act
entitled "Offences"

Privacy offences

65.4 (1) An individual, other than an individual who is a service provider or an employee or associate of a service provider, who wilfully does any of the following commits an offence:

(a) collects personal information except as authorized by Part 3;

(b) uses personal information except as authorized by Part 3;

(c) discloses personal information except as authorized by Part 3;

(d) fails to notify the head of a public body of unauthorized disclosure as required by Part 3.

(2) A service provider or an employee or associate of a service provider who does any of the following commits an offence:

(a) collects personal information except as authorized by Part 3;

(b) uses personal information except as authorized by Part 3;

(c) discloses personal information except as authorized by Part 3;

(d) fails to notify the head of a public body of unauthorized disclosure as required by Part 3;

(e) dismisses, suspends, demotes, disciplines, harasses or otherwise disadvantages an employee, or denies the employee a benefit, because the employee has done, or the employer believes that the employee will do, anything described in section 30.3 (b) to (d).

(3) A service provider commits an offence if an employee or associate of the service provider commits any of the offences under subsection (2).

(4) It is a defence to a charge under subsections (2) and (3) if the person charged demonstrates that the person exercised due diligence to avoid committing the offence.

Corporate liability

65.5 If a corporation commits an offence under section 65.3 or 65.4, an officer, director or agent of the corporation who authorizes, permits or acquiesces in the commission of the offence also commits an offence, whether or not the corporation is prosecuted for the offence.

Cont'd

Page 263 of 513

Withheld pursuant to/removed as

s.13

Section 37 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

adds a new Part 5.1 to the
Freedom of Information and Protection of Privacy Act
entitled "Offences"

Penalties

65.6 (1) A person who commits an offence under section 65.2 is liable on conviction to a fine of up to $50 000.

(2) A person who commits an offence under section 65.3 or 65.4 is liable on conviction,

(a) in the case of an individual, other than an individual who is a service provider, to a fine of up to $50 000,

(b) subject to paragraph (c), 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

(c) in the case of a corporation, to a fine of up to $500 000.

Time limit for laying an information to commence a prosecution

65.7 (1) The time limit for laying an information to commence a prosecution for an offence under sections 65.3 and 65.4 is

(a) one year after the date on which the act or omission that is alleged to constitute the offence occurred, or

(b) if the minister responsible for this Act issues a certificate described in subsection (2), one year after the date on which the minister learned of the act or omission referred to in paragraph (a) of this subsection.

(2) A certificate issued by the minister responsible for this Act certifying the date referred to in subsection (1) (b) is proof of that date.

.

Leave this page blank

Section 38 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 69 of the
Freedom of Information and Protection of Privacy Act

General information respecting use of personal information

69 (1) In this section:

"personal information bank" means ~~a collection of~~ an aggregation of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual

69 (3) The personal information directory must include a summary that meets the requirements of the minister responsible for this Act of the following information:

(a) the personal information banks that are ~~in the custody or control of~~ in the custody or under the control of each ministry of the government of British Columbia;

(5) The head of a ministry ~~must conduct a privacy impact assessment in accordance with the directions of the minister~~ must conduct a privacy impact assessment and must do so in accordance with the directions of the minister responsible for this Act.

(5.2) If the minister responsible for this Act receives a privacy impact assessment under subsection (5.1) respecting a common or integrated program or activity ~~or a data-linking initiative~~, the minister must submit, during the development of the proposed enactment, system, project, program or activity, the privacy impact assessment to the commissioner for the commissioner's review and comment.

(5.3) The head of a public body that is not a ministry ~~must conduct a privacy impact assessment in accordance with the directions of the minister~~ must conduct a privacy impact assessment and must do so in accordance with the directions of the minister responsible for this Act.

(5.4) The head of a public body that is not a ministry, with respect to a proposed system, project, program or activity, must submit, during the development of the proposed system, project, program or activity, the privacy impact assessment, if it addresses a common or integrated program or activity ~~or a data-linking initiative~~, to the commissioner for the commissioner's review and comment.

(5.5) The head of a public body must notify the commissioner ~~of a data-linking initiative or~~ of a common or integrated program or activity at an early stage of developing the initiative, program or activity. **Cont'd**

Page 267 of 513

Withheld pursuant to/removed as

s.13

Section 38 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

Amends section 69 of the
Freedom of Information and Protection of Privacy Act

Cont'd

General information respecting use of personal information

~~**69** (5.6) If all the participants in a data-linking initiative are either a health care body, the ministry of the minister responsible for the administration of the *Ministry of Health Act* or a health-related organization as prescribed, then~~

~~(a) subsections (5.3), (5.4) and (5.5) do not apply with respect to a participant that is a health care body or a health-related organization as prescribed, and~~

~~(b) subsections (5), (5.1) and (5.5) do not apply with respect to a participant that is the ministry of the minister responsible for the administration of the *Ministry of Health Act*.~~

~~(8) Not later than 60 days after making an order under section 33.1 (3) *[orders allowing disclosure outside Canada]*, the minister responsible for this Act must publish a summary of the order.~~

(5.10) The minister responsible for this Act may, under subsections (5) or (5.3), give different directions for different categories of personal information.

Page 269 of 513

Withheld pursuant to/removed as

s.13

Section 39 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 69.1 of the
Freedom of Information and Protection of Privacy Act

Public information regarding health information banks

69.1 (3) For the purposes of subsection (2), the personal information directory must include the following information in accordance with the requirements of the minister responsible for this Act:

(a) the provisions of the order under section 3 *[establishment or designation of health information banks]* of the *E-Health (Personal Health Information Access and Protection of Privacy) Act* in relation to each health information bank that is ~~in the custody or control of~~ in the custody or under the control of each health care body;

(b) a summary of the health information-sharing agreements into which each health care body has entered;

(c) any other information the minister responsible for this Act considers appropriate.

~~(5) A ministry that is a health care body must conduct a privacy impact assessment that is in relation to~~

~~(a) a health information bank in its custody or control, or~~
~~(b) a health information-sharing agreement to which it is a party in accordance with the directions of the minister responsible for this Act.~~

(5) A ministry that is a health care body must conduct a privacy impact assessment, and must do so in accordance with the directions of the minister responsible for this Act, in relation to

(a) a health information bank in its custody or under its control, and

(b) a health information-sharing agreement to which it is a party.

(6) The minister responsible for this Act may, under subsection (5), give different directions for different categories of personal information.

Page 271 of 513

Withheld pursuant to/removed as

s.13

Section 40 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces section 70 of the
Freedom of Information and Protection of Privacy Act

~~**Policy manuals available without request**~~

~~**70** (1) The head of a public body must make available to the public, without a request for access under this Act,~~

~~(a) manuals, instructions or guidelines issued to the officers or employees of the public body, or~~

~~(b) substantive rules or policy statements adopted by the public body,~~

~~for the purpose of interpreting an enactment or of administering a program or activity that affects the public or a specific group of the public.~~

~~(2) The head of a public body may delete from a record made available under this section any information he or she would be entitled to refuse to disclose to an applicant.~~

~~(3) If information is deleted, the record must include a statement of~~ […..]

Certain records available without request

70 (1) The head of a public body must make available to the public, without a request for access under this Act, the following records if they were created for the purpose of interpreting an enactment or for the purpose of administering a program or activity that affects the public:

(a) manuals, instructions or guidelines issued to the officers or employees of the public body;

(b) substantive rules or policy statements adopted by the public body.

(2) The head of a public body may sever from a record made available under this section any information the head of the public body would be entitled under Part 2 of this Act to refuse disclose to an applicant.

(3) If information is severed from a record, the record must include a statement of

(a) the fact that information has been severed from the record,

(b) the nature of the information severed from the record, and

(c) the reason for severing the information from the record.

(4) The head of a public body may require a person who asks for a copy of a record made available under this section to pay a fee to the public body.

Page 273 of 513

Withheld pursuant to/removed as

s.13

Section 41 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 71 of the
Freedom of Information and Protection of Privacy Act

Records available without request

71 (1) Subject to subsection (1.1), the head of a public body must establish categories of records that are in the custody or under the control of the public body and are available to the public without a request for access under this Act.

(1.1) The head of a public body must not establish a category of records that contain personal information unless the information

(a) may be disclosed under ~~section 33.1 or 33.2~~ section 33, or

(b) would not constitute, if disclosed, an unreasonable invasion of the personal privacy of the individual the information is about.

(1.2) Section 22 (2) to (4) applies to the determination of unreasonable invasion of personal privacy under subsection (1.1) (b) of this section.

(1.3) The head of a public body may sever from a record made available under this section any information the head of the public body would be entitled under Part 2 of this Act to refuse to disclose to an applicant.

(1.4) If information is severed from a record, the record must include a statement of

(a) the fact that information has been severed from the record,

(b) the nature of the information severed from the record, and

(c) the reason for severing the information from the record.

(2) The head of a public body may require a person who asks for a copy of an available record to pay a fee to the public body.

(3) Subsection (1) does not limit the discretion of the government of British Columbia or a public body to disclose records that do not contain personal information.

Page 275 of 513

Withheld pursuant to/removed as

s.13

Section 42 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 71.1 of the
Freedom of Information and Protection of Privacy Act

Records that ministries must disclose

71.1 (1) Subject to subsection (2), the minister responsible for this Act may establish categories of records that are in the custody or under the control of one or more ministries and are available to the public without a request for access under this Act.

(2) The minister responsible for this Act must not establish a category of records that contain personal information unless the information

(a) may be disclosed under ~~section 33.1 or 33.2~~ section 33, or

(b) would not constitute, if disclosed, an unreasonable invasion of the personal privacy of the individual the information is about.

(3) Section 22 (2) to (4) applies to the determination of unreasonable invasion of personal privacy under subsection (2) (b) of this section.

(4) The minister responsible for this Act may require one or more ministries to disclose a record that is within a category of records established under subsection (1) of this section or section71 (1).

(5) If required to disclose a record under subsection (4), a ministry must do so in accordance with any directions issued relating to the disclosure by the minister responsible for this Act.

(6) The head of a public body may sever from a record made available under this section any information the head of the public body would be entitled under Part 2 of this Act to refuse to disclose to an applicant.

(7) If the information is severed from a record, the record must include a statement of
a) the fact that information has been severed from the record,
b) the nature of the information severed from the record, and
c) the reason for severing the information from the record.

Page 277 of 513

Withheld pursuant to/removed as

s.13

Section 43 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals section 74 and 74.1 of the
Freedom of Information and Protection of Privacy Act

~~**General offences and penalties**~~

~~**74** (1) A person must not wilfully do any of the following:~~

~~(a) make a false statement to, or mislead or attempt to mislead, the commissioner or another person in the performance of the duties, powers or functions of the commissioner or other person under this Act;~~

~~(b) obstruct the commissioner or another person in the performance of the duties, powers or functions of the commissioner or other person under this Act;~~

~~(c) fail to comply with an order made by the commissioner under section 54.1 or 58 or by an adjudicator under section 65 (2).~~

~~(2) A person who contravenes subsection (1) commits an offence and is liable to a fine of up to $5 000.~~

~~(3) Section 5 of the Offence Act does not apply to this Act.~~

~~**Privacy protection offences**~~

~~**74.1** (1) A person who contravenes section 30.4 [unauthorized disclosure] or 30.5 [notification of unauthorized disclosure] commits an offence.~~

~~(2) A person who is a service provider or an employee or associate of a service provider commits an offence if the person does any of the following:~~

> ~~(a) stores or allows access to personal information to which section 30.1 [location and access in Canada] applies contrary to that section;~~
> ~~(b) contravenes section 30.2 [obligation to report foreign demand for disclosure];~~
> ~~(c) contravenes section 30.3 [whistle-blower protection].~~

~~(3) If an employee or associate of a service provider~~

> ~~(a) stores or allows access to personal information to which section 30.1 applies contrary to that section,~~
> ~~(b) contravenes section 30.2,~~
> ~~(c) contravenes section 30.3,~~
> ~~(d) contravenes section 30.4, or~~
> ~~(e) contravenes section 30.5~~,….[see Appendix for full repeal]

Page 279 of 513

Withheld pursuant to/removed as

s.13

Section 44 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces section 75 of the
Freedom of Information and Protection of Privacy Act

[see Appendix for repeal]

Fees

75 (1) The head of a public body may require an applicant who makes a request under section 5 to pay to the public body the following:

(a) a prescribed application fee;

(b) prescribed fees for the following services:

(i) locating and retrieving the record;

(ii) producing the record;

(iii) preparing the record for disclosure, except for time spent severing information from the record;

(iv) shipping and handling the record;

(v) providing a copy of the record.

(2) Subsection (1) (b) (i) does not apply to the first 3 hours spent on a request.

(3) Subsection (1) does not apply to a request for the applicant's own personal information.

(4) If an applicant is required to pay fees for services under subsection (1) (b), the head of the public body

(a) must give the applicant a written estimate of the total fees before providing the services, and

(b) may require the applicant to pay a deposit in an amount set by the head of the public body.

(5) If the head of a public body receives an applicant's written request to excuse payment of all or part of the fees required under subsection (1) (b), the head of the public body may excuse payment, if, in the head of the public body's opinion,

(a) the applicant cannot afford the payment or for any other reason it is fair to excuse payment, or

(b) the record relates to a matter of public interest, including the environment or public health or safety.

(6) The head of a public body must respond to a request under subsection (5) in writing and within 20 days after receiving the request.

(7) The fees that prescribed categories of applicants are required to pay for services under subsection (1) (b) may differ from the fees other applicants are required to pay for the services but may not be greater than the actual costs of the services.

Page 281 of 513

Withheld pursuant to/removed as

s.13

Section 45 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 76 of the
Freedom of Information and Protection of Privacy Act

Power to make regulations

76 (2) Without limiting subsection (1), the Lieutenant Governor in Council may make regulations as follows:

(h) prescribing the classes of individuals who may act for minors, ~~incompetents~~ deceased persons or any other individuals under this Act and regulating the manner in which, and the extent to which, any rights or powers of individuals under this Act may be exercised on their behalf;

(i.1) prescribing an application fee and fees for services;

(2.1) The Lieutenant Governor in Council, after consultation with the commissioner, may make regulations as follows:

(a) for the purposes of section 26 (d);
~~(b) for the purposes of section 36.1 (1), respecting how data-linking initiatives must be carried out~~
(b) for the purposes of section 36.1

(i) establishing how data-linking programs must be conducted, and
(ii) exempting a data-linking program or class of data-linking program from regulations made under subparagraph (i) of this paragraph.

Page 283 of 513

Withheld pursuant to/removed as

s.13

Section 46 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 76.1 of the
Freedom of Information and Protection of Privacy Act

Ministerial regulation making power

76.1 (1) The minister responsible for this Act may, by regulation, amend Schedule 2 to do one or more of the following:

(a) add to it any agency, board, commission, corporation, office or other body

(i) of which any ~~member~~ member, director, officer is appointed by the Lieutenant Governor in Council or a minister,

(ii) of which a controlling interest in the share capital is owned by the government of British Columbia or any of its ~~agencies, or~~ agencies or a public body;

(iii) that performs functions under an ~~enactment~~ enactment, or

(iv) if the minister responsible for this Act determines that it would be in the public interest to add the agency, board, commission, corporation, office or other body to Schedule 2;

(b) designate or change the designation of the head of a public body;

(c) ~~delete~~ remove from it an agency, board, commission, corporation, office or other body that

(i) no longer exists, or

(ii) no longer meets the criteria established by paragraph (a).

(2) The minister responsible for this Act may, by regulation, amend Schedule 3 to do one or more of the following:

(a) add to it the name of the governing body of a profession or occupation if

(i) any member of that body is appointed by the Lieutenant Governor in Council, a minister or an Act, or

(ii) the profession or occupation is governed under an Act;

(b) ~~delete~~ remove from it a governing body that

(i) no longer exists, or

(ii) no longer meets the criteria established by paragraph (a).

(3) The minister responsible for this Act may make regulations establishing measures that must be taken by a public body in relation to respecting programs, projects and systems in which the public body discloses personal information outside of Canada.

Page 285 of 513

Withheld pursuant to/removed as

s.13

Section 47 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals section 79 of the
Freedom of Information and Protection of Privacy Act

~~**Relationship of Act to other Acts**~~

~~**79** If a provision of this Act is inconsistent or in conflict with a provision of another Act, the provision of this Act prevails unless the other Act expressly provides that it, or a provision of it, applies despite this Act.~~

Page 287 of 513

Withheld pursuant to/removed as

s.13

Section 48 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends Schedule 1 of the
Freedom of Information and Protection of Privacy Act
by repealing and replacing the definition of "aboriginal government" and adding a definition of "Indigenous governing entity"

Definitions

In this Act:

~~**"aboriginal government"** means an aboriginal organization exercising governmental functions;~~

"Indigenous governing entity" means an Indigenous entity that exercises governmental functions, and includes but is not limited to an Indigenous governing body as defined in the *Declaration on the Rights of Indigenous Peoples Act*;

Page 289 of 513

Withheld pursuant to/removed as

s.13

Section 48 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends Schedule 1 of the
Freedom of Information and Protection of Privacy Act
by repealing the definition of "access"

Definitions

In this Act:

~~**"access"** means, for the purposes of Part 3, disclosure of personal information by the provision of access to personal information;~~

Page 291 of 513

Withheld pursuant to/removed as

s.13

Section 48 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends Schedule 1 of the
Freedom of Information and Protection of Privacy Act
by amending the definition of "agency"

Definitions

In this Act:

"agency" means, ~~for the purposes of sections 33.2 (d) and 36.1 (3) (b) (i)~~ for the purposes of section 33 (2) (k) and the definitions of "common or integrated program or activity" and "~~data-linking initiative~~ data-linking program",

Page 293 of 513

Withheld pursuant to/removed as

s.13

Section 48 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends Schedule 1 of the
Freedom of Information and Protection of Privacy Act
by repealing and replacing definitions related to data linking

Definitions

In this Act

~~**data linking"** means the linking or combining of personal information in one database with personal information in one or more other databases if the purpose of the linking or combining is different from~~

~~(a) the purpose for which the information in each database was originally obtained or compiled, and~~

~~(b) every purpose that is consistent with each purpose referred to in paragraph (a);~~

~~**"data-linking initiative"** means a new or newly revised enactment, system, project, program or activity that has, as a component, data linking between~~

~~(a) two or more public bodies, or~~

~~(b) one or more public bodies and one or more agencies;~~

"**common key**" means information about an identifiable individual that is common to 2 or more data sets;

"**data-linking**" means the linking, temporarily or permanently, of 2 or more data sets using one or more common keys;

"**data-linking program**" means a program of a public body that involves data-linking if at least one data set in the custody or under the control of a public body is linked with a data set in the custody or under the control of one or more other public bodies or agencies without the consent of the individuals whose personal information is contained in the data set;

"**data set**" means an aggregation of information that contains personal information;

Page 295 of 513

Withheld pursuant to/removed as

s.13

Section 48 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends Schedule 1 of the
Freedom of Information and Protection of Privacy Act
by removing the reference to "Provincial auxiliary hospital"

Definitions

In this Act

"health care body" means

(a) a hospital as defined in section 1 of the Hospital Act,

~~(b) a Provincial auxiliary hospital established under the *Hospital (Auxiliary) Act*,~~

(c) a regional hospital district and a regional hospital district board under the Hospital District Act,

Page 297 of 513

Withheld pursuant to/removed as

s.13

Section 48 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends Schedule 1 of the
Freedom of Information and Protection of Privacy Act
by adding the definition of Indigenous peoples

"Indigenous peoples" has the same meaning as in the Declaration on the Rights of Indigenous Peoples Act;

Page 299 of 513

Withheld pursuant to/removed as

s.13

Section 48 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends Schedule 1 of the
Freedom of Information and Protection of Privacy Act
by repealing and replacing the definition of "intimate partner"

Definitions

In this Act

~~**"intimate partner"** includes, with respect to an individual,~~

~~(a) a current or former spouse of the individual, by marriage or common law,~~
~~(b) a current or former boyfriend or girlfriend of the individual, and~~
~~(c) an individual referred to in paragraph (a) or (b) who is the same gender as the individual;~~

"intimate partner" means, with respect to an individual, any of the following:

(a) an individual who is or was a spouse, dating partner or sexual partner of the individual;

(b) an individual who is or was in a relationship with the individual that is similar to a relationship described in paragraph (a);

Page 301 of 513

Withheld pursuant to/removed as

s.13

Section 48 ***of the Freedom of Information and Protection of Privacy Amendment Act, 2021***

amends Schedule 1 of the
Freedom of Information and Protection of Privacy Act
by repealing the definition of "social media site"

Definitions

In this Act

~~**"social media site"** means the Internet site referred to as Facebook, YouTube, Twitter or MySpace or a prescribed social media site;~~

Page 303 of 513

Withheld pursuant to/removed as

s.13

Section 49 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends Schedule 2 of the
Freedom of Information and Protection of Privacy Act
by adding police associations

Public Bodies

Public Body:	BC Association of Chiefs of Police
Head:	President
Public Body:	BC Association of Municipal Chiefs of Police
Head:	President

Page 305 of 513

Withheld pursuant to/removed as

s.13

Section 50 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

Amends Schedule 2 of the
Freedom of Information and Protection of Privacy Act
by removing "Office of the Premier"

Public Bodies

~~Public Body: Office of the Premier and Executive Council Operations~~

~~Head: Premier~~

Page 307 of 513

Withheld pursuant to/removed as

s.13

Section 51 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

Transitional Provisions

Transition – data-linking programs

74 A data-linking initiative that started before section 24 of this Act is brought into force is subject to section 36.1 of the *Freedom of Information and Protection of Privacy Act* as it read before the coming into force of section 24 of this Act.

Page 309 of 513

Withheld pursuant to/removed as

s.13

Section 52 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 68 (4) (a) of the
Assessment Act

Protection of privacy in assessment roll and records

68 (4) Subsections (1) and (3) do not apply to an assessment roll or record that is supplied

(a) to a person or for a purpose specified in ~~section 33.1 or 33.2~~ section 33 of the *Freedom of Information and Protection of Privacy Act*,

Page 311 of 513

Withheld pursuant to/removed as

s.13

Section 53 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 74 (2) of the
Child, Family and Community Service Act

Freedom of Information and Protection of Privacy Act

74 (2) For the purpose of its application to this Act, the *Freedom of Information and Protection of Privacy Act* is deemed to be modified as follows:

[…..]

(e) the only provisions of sections 33 that apply to a director are the following:

(i) section 33 (2) (a) *[in accordance with Part 2]*;

(ii) section 33 (2) (c) *[individual consent]*;

(iii) section 33 (2) (j) [evaluating program or activity];

(iv) section 33 (2) (k) [common or integrated program or activity];

(v) section 33 (2) (p) [payment to government or a public body];

(vi) section 33 (3) (b) [domestic violence];

(vii) section 33 (3) (g) [to archives for archival purposes];

(viii) section 33 (3) (h) [research purposes];

(ix) section 33 (4) [by archives for archival or historical purposes];

(x) section 33 (8) [identity management services], except that the reference to "any other provision of this section" is to be read as a reference to any provision referred to in subparagraph (i) to (vi) and (viii) to (x) of this paragraph;,

(e.1) the authority for a public body to disclose personal information under ~~section 33.1 (1) (q) or (r) or (7) or 33.3~~ section 33.1 (2) (r) or (w) or 33.3 does not include the authority to disclose information that could reasonably be expected to reveal that

(i) a child is a child in care, or

(ii) an individual is an individual who has made a report under section 14 of this Act;

Page 313 of 513

Withheld pursuant to/removed as

s.13

Section 54 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 79 of the
Child, Family and Community Service Act

Disclosure without consent

79 A director may, without the consent of any person, disclose information obtained under this Act if the disclosure is

[….]

(j) ~~made in Canada to~~ made to caregivers or prospective adoptive parents and the information relates to children in their care, or

(k) ~~made in Canada and necessary~~ necessary for the administration of this Act.

Page 315 of 513

Withheld pursuant to/removed as

s.13

Section 55 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals section 86 (2) of the *Civil Resolution Tribunals Act*

Protection of personal information

86 ~~(2) The tribunal must ensure that personal information in its custody or under its control is stored only in Canada.~~

Page 317 of 513

Withheld pursuant to/removed as

s.13

Section 56 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 6 (3) of the *Criminal Records Review Act*

Use of information

6 (3) Information provided under this Act must not be used or disclosed for any purpose other than the purpose set out in section 2 of this Act or in ~~section 33.1 (1) (m), 33.2 (i) or~~ section 33 (3) (a) or (d) or 44 (2) or (3) of the *Freedom of Information and Protection of Privacy Act*.

Page 319 of 513

Withheld pursuant to/removed as

s.13

Section 57 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 10 (1) (b) of the
E-Health (Personal Health Information Access and Protection of Privacy) Act

Effect of disclosure directives

10 (1) A person who is otherwise permitted to collect, use or disclose personal health information from a health information bank must not do so in any manner that is inconsistent with a disclosure directive except as follows:

(a) to notify a person that a disclosure directive applies to personal health information that would otherwise be available to the person;

(b) for a purpose described in section ~~33.1 (1) (c)~~ section 33 (2) (e) of the *Freedom of Information and Protection of Privacy Act*;

(c) with the express consent of the person who made the disclosure directive;

(d) if section 12 *[exception — urgent or emergency health care]* of the *Health Care (Consent) and Care Facility (Admission) Act* applies and a health care provider acting under that section reasonably believes that the personal health information may be required to provide health care in accordance with that section.

Page 321 of 513

Withheld pursuant to/removed as

s.13

Section 58 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 18 of the
E-Health (Personal Health Information Access and Protection of Privacy) Act

Purposes for which disclosure always authorized

18 (1) An administrator may disclose personal health information inside Canada from a health information bank for one or more of the following purposes:

(a) a purpose described in ~~section 33.2 (f) and (i)~~ section 33 (2) (s) and (3) (d) of the *Freedom of Information and Protection of Privacy Act*;

(b) to investigate or discipline a person regulated by a governing body of a health profession that has authority, under an enactment, to investigate or discipline the person;

(c) to monitor, by a governing body of a health profession, the practice of a health profession that is, under an enactment, regulated by that body;

(d) a purpose for which the person who is the subject of the personal health information has expressly consented.

(2) An administrator may disclose personal health information inside or outside Canada from a health information bank for one or more of the following purposes:

(a) a purpose described in section ~~33.1 (1) (a), (c), (e), (e.1), (g), (i), (i.1), (m), (m.1), (n), (p), (p.1), (p.2) or (t), (6) or (7)~~ section 33 (2) (a), (e), (h), (l), (m), (o), (p), (t), (u) or (v), (3) (a), (b), or (c), (8) or (9) of the *Freedom of Information and Protection of Privacy Act*, or

(b) a purpose for which the person who is the subject of the personal health information has expressly consented in writing.

Page 323 of 513

Withheld pursuant to/removed as

s.13

Section 59 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 19 of the
E-Health (Personal Health Information Access and Protection of Privacy) Act

Information-sharing agreements required for disclosure

19 (1) Personal health information contained in a health information bank may be disclosed only if

(a) disclosure is authorized by the terms of the designation order that relates to the health information bank,

(b) the administrator of the health information bank enters into an information-sharing agreement under this section, and

(c) if personal health information is to be disclosed on a bulk or regular basis, it is disclosed only to one or more of the following persons:

(i) an agency or ministry of the government of British Columbia, of another province or of Canada, including a Crown corporation;
(ii) a health care body;
(iii) an ~~aboriginal government~~ Indigenous governing entity, an educational body or a social services body, as those terms are defined in the *Freedom of Information and Protection of Privacy Act*;
(iv) a public body in another jurisdiction of Canada that is equivalent to one described in subparagraphs (ii) and (iii);
(v) a health service provider;
(vi) a body responsible for the regulation of health professionals;
(vii) an association of health professionals;
(viii) a prescribed body that is public in nature.

Page 325 of 513

Withheld pursuant to/removed as

s.13

Section 60 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 90 (9) of the
Employer Health Tax Act

Communication of information

90 (9) To the extent of any inconsistency or conflict with ~~sections 32 [use of personal information], 33 [disclosure of personal information], 33.1 [disclosure inside or outside Canada] and 33.2 [disclosure inside Canada only]~~ sections 32 [use of personal information] and 33 [disclosure of personal information] of the Freedom of Information and Protection of Privacy Act, this section applies despite that Act

Page 327 of 513

Withheld pursuant to/removed as

s.13

Section 61 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 30 (2.3) of the
Employment and Assistance Act

Agreements

30 (2.3) An information-sharing agreement under this section is not required for the purpose of sharing for research purposes personal information collected under this Act if the personal information is disclosed in accordance with ~~section 35~~ section 33 (3) (h) of the *Freedom of Information and Protection of Privacy Act*.

Page 329 of 513

Withheld pursuant to/removed as

s.13

Section 62 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 21 (2.3) of the
Employment and Assistance for Persons with Disabilities Act

Agreements

21 (2.3) An information-sharing agreement under this section is not required for the purpose of sharing for research purposes personal information collected under this Act if the personal information is disclosed in accordance with ~~section 35~~ section 33 (3) (h) of the *Freedom of Information and Protection of Privacy Act*.

Page 331 of 513

Withheld pursuant to/removed as

s.13

Section 63 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 243 (4) (c) of the
Family Law Act

Restrictions on disclosure of information

243 (4) This section does not apply to

(a) personal information, as defined in the *Freedom of Information and Protection of Privacy Act*, that has been in existence for 100 years or more,

(b) information not described by paragraph (a) that has been in existence for 50 years or more, or

(c) information for research purposes disclosed under ~~section 33.1 (1) (s)~~ section 33 (3) (h) of the *Freedom of Information and Protection of Privacy Act*.

Page 333 of 513

Withheld pursuant to/removed as

s.13

Section 64 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 43 (2) of the
Family Maintenance Enforcement Act

Information confidential

43 (2) Subsection (1) does not apply to information for research purposes disclosed in accordance with ~~section 33.1 (1) (s)~~ section 33 (3) (h) of the *Freedom of Information and Protection of Privacy Act*.

Ministry of Citizens' Services
Amendments to the *Freedom of Information and Protection of Privacy Act* (FOIPPA)

Section Notes

Section 64 **amends subsection 43 (2) of** the *Family Maintenance Enforcement Act* (FMEA)

Purpose:

- This amendment strikes out the phrase "section 33.1 (1) (s)" and substitutes "section 33 (3) (h)" in subsection 43 (2) of the FMEA.

Existing Provision:

- Section 43 (2) of the FMEA refers to a section in FOIPPA that is being repealed, replaced and re-numbered as a result of changes made as part of this Bill.

Significance:

- This is a consequential amendment made necessary by section 21 of this Bill, which repeals and replaces sections 33.1 of FOIPPA with a new consolidated section 33.

Section 65 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 64 (8) of the
Income Tax Act

Communication of information and related offences

64 (8) To the extent of any inconsistency or conflict with ~~sections 32, 33, 33.1 and 33.2~~ sections 32 and 33 of the *Freedom of Information and Protection of Privacy Act*, this section applies despite that Act.

Page 337 of 513

Withheld pursuant to/removed as

s.13

Section 66 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 6.1 (2) of the
Ministry of Environment Act

Disclosure of information

6.1 (2) In accordance with ~~section 33.1 (1) (c)~~ section 33 (2) (e) of the *Freedom of Information and Protection of Privacy Act*, the minister may disclose the following information ~~inside or outside Canada~~ with respect to a person who is convicted of an offence, has paid or is liable to pay an administrative penalty or is subject to another sanction under an enactment:

(a) the name of the person;
(b) the provision of the enactment that the person contravened or under which a sanction has been imposed;
(c) the location at which the contravention occurred or the conduct or circumstances that resulted in the sanction arose;
(d) a description of the contravention or the conduct or circumstances that resulted in the sanction;
(e) the fine, sentence, administrative penalty or other sanction to which the person is subject;
(f) if a fine or administrative penalty is overdue, the date it was due and the outstanding amount.

Page 339 of 513

Withheld pursuant to/removed as

s.13

Section 67 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 23 of the
Pharmaceutical Services Act

Disclosure of personal information

23 (1) The minister may disclose, inside Canada, personal information under this Act for one or more of the following purposes:

(a) for a purpose described in ~~section 33.2 (f) or (i)~~ section 33 (2) (s) or (3) (d) of the *Freedom of Information and Protection of Privacy Act* only;

(b) to investigate or discipline a person regulated by a governing body of a health profession that has authority, under an enactment of any jurisdiction, to investigate or discipline the person;

(c) to monitor, by a governing body of a health profession, the practice of a health profession that is, under an enactment of any jurisdiction, regulated by that body;

(d) for a purpose to which the person who is the subject of the personal information has consented.

(2) The minister may disclose personal information under this Act inside or outside Canada for one or more of the following purposes:

(a) for a purpose described in ~~section 33.1 (1) (a), (c), (e), (e.1), (g), (i), (i.1), (m), (m.1), (n), (p), (p.1), (p.2) or (t), (6) or (7)~~ section 33 (2) (a), (e), (h), (l), (m), (o), (p), (t), (u) or (v), (3) (a), (b) or (c), (8) or (9) of the *Freedom of Information and Protection of Privacy Act* only;

(b) for a purpose to which the person who is the subject of the personal information has consented in writing.

Page 341 of 513

Withheld pursuant to/removed as

s.13

Section 68 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 29 (1) (b) of the
Pharmaceutical Services Act

Effect of protective words

29 (1) A person within a prescribed class of persons who is otherwise permitted under this Act to collect, use or disclose personal information from prescribed information management technology must not do so if a protective word is attached to the personal information, except as follows:

(a) to notify a person that a protective word applies to personal information that would otherwise be available to the person;

(b) for a purpose described in ~~section 33.1 (1) (c)~~ section 33 (2) (e) of the *Freedom of Information and Protection of Privacy Act*;

(c) with the express consent of the person to whose personal information the protective word applies;

(d) if section 12 of the *Health Care (Consent) and Care Facility (Admission) Act* applies and a health care provider acting under that section reasonably believes that the personal information may be required to provide health care in accordance with that section.

Page 343 of 513

Withheld pursuant to/removed as

s.13

Section 69 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 182 of the
Police Act

***Freedom of Information and Protection of Privacy Act* does not apply**

182 ~~Except as provided by this Act and by section 3 (3)~~ Except as provided by this Act and section 3 (4) of the *Freedom of Information and Protection of Privacy Act*, that Act does not apply to

(a) any record of a complaint concerning the conduct of a member that is made, submitted, registered or processed under this Part,

(b) any record related to a record described in paragraph (a), including, without limitation, any record related to a public hearing or review on the record in respect of the matter,

(c) any information or report in respect of which an investigation is initiated under this Part, or

(d) any record related to information or a report described in paragraph (c), including, without limitation, any record related to a public hearing or review on the record in respect of the matter,

whether that record, information or report is created on or after a complaint is made, submitted or registered or the investigation is initiated, as the case may be.

Page 345 of 513

Withheld pursuant to/removed as

s.13

Section 70 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends subsection 170.2 (5) (b) of the
School Act

Public post-secondary students

170.2 (5) The personal information of a student obtained under this section by the minister responsible for public post-secondary institutions may be used only for the following purposes:

(a) conducting research and statistical analysis relating to students, including research and analysis as authorized under the *Freedom of Information and Protection of Privacy Act*;

(b) delivering a common or integrated program or activity within the meaning of ~~section 33.2 (d)~~ section 33 (2) (k) of the *Freedom of Information and Protection of Privacy Act*;

(c) facilitating the administration of the BC Student Assistance Program by the minister responsible for the program;

(d) conducting research and statistical analysis related to the BC Student Assistance Program;

(e) evaluating the effectiveness of the BC Student Assistance Program.

Page 347 of 513

Withheld pursuant to/removed as

s.13

Section 71 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

repeals and replaces section 49 of the
Secure Care Act

~~***49 Section 3 (1) of the Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, is amended by adding the following paragraph:***~~

~~(c.2) a record that is created by or for, or is in the custody or control of, the Secure Care Board and that relates to the exercise of that board's functions under the *Secure Care Act*;.~~

49 *Section 3 (3) of the Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, is amended by adding the following paragraph:*

(g.1) a record that is created by or for, or is in the custody or under the control of, the Secure Care Board and that relates to the exercise of that board's functions under the *Secure Care Act*;

Page 349 of 513

Withheld pursuant to/removed as

s.13

Section 72 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 120 (10) of the
Speculation and Vacancy Tax Act

Communication of information

120 (10) To the extent of any inconsistency or conflict with ~~sections 32 *[use of personal information]*, 33 *[disclosure of personal information]*, 33.1 *[disclosure inside or outside Canada]* and 33.2 *[disclosure inside Canada only]*~~ sections 32 [use of personal information] and 33 [disclosure of personal information] of the *Freedom of Information and Protection of Privacy Act*, this section applies despite that Act.

Page 351 of 513

Withheld pursuant to/removed as

s.13

Section 73 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

amends section 41.1 (2) (b) of the
Vital Statistics Act

Information-sharing agreements

41.1 (2) The registrar general may enter into an information-sharing agreement under subsection (1) only with the following bodies:

(a) an agency or ministry of the government of British Columbia, of another province, or of Canada, including a Crown corporation;

(b) an ~~aboriginal government~~ Indigenous governing entity, an educational body, a health care body or a social services body, as those terms are defined in the *Freedom of Information and Protection of Privacy Act*;

(c) a public body in another jurisdiction of Canada that is equivalent to one described in paragraph (b);

(d) a prescribed body that is public in nature.

Page 353 of 513

Withheld pursuant to/removed as

s.13

Section 74 of the *Freedom of Information and Protection of Privacy Amendment Act, 2021*

Commencement

The provisions of this Act referred to in column 1 of the following table come into force as set out in column 2 of the table:

Item	Column 1 **Provisions of Act**	Column 2 **Commencement**
1	Anything not elsewhere covered by this table	The date of Royal Assent
2	Section 25	By regulation of the Lieutenant Governor in Council
3	Section 49	By regulation of the Lieutenant Governor in Council

Page 355 of 513

Withheld pursuant to/removed as

s.13

RE: UPDATED: KMQA doc, now with scripts

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To: Youngs, Kirsten R GCPE:EX, Scott, Samantha CITZ:EX
Sent: October 13, 2021 5:02:25 PM PDT

Thanks, Kirsten. This and all updated materials have been provided to MLB for tomorrow's prep session.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Sent: October 13, 2021 4:27 PM
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Subject: UPDATED: KMQA doc, now with scripts

I understand we are waiting on a couple data facts from program for the attached, but Shauna has approved if you need to add these to the binder asap.

From: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>
Sent: October 13, 2021 3:14 PM
To: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>; Harriman, Rheannon CITZ:EX <Rheannon.Harriman@gov.bc.ca>
Cc: Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>; Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>
Subject: RE: UPDATED: KMQA doc, now with scripts, for review

These 5 look good thx!

From: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Sent: October 13, 2021 11:55 AM
To: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>; Harriman, Rheannon CITZ:EX <Rheannon.Harriman@gov.bc.ca>
Cc: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>; Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>
Subject: UPDATED: KMQA doc, now with scripts, for review

Hello team!
Thank you to Kerry for the call this a.m. As requested, I've moved the five topic 'scripts' to the top and utilised the existing KMs for your review. A few highlighted details to come from Hayden/Matt as I understand it, but I think it's looking really good.
I'll work on the OIPC doc KMs this afternoon, let me know if that one has been updated since our meeting?
Jeremy is working on the NR+BG updates (thank you Jeremy!)
KY

From: Youngs, Kirsten R GCPE:EX
Sent: October 12, 2021 6:30 PM
To: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>; Harriman, Rheannon CITZ:EX <Rheannon.Harriman@gov.bc.ca>
Cc: Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>; Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>
Subject: UPDATED: KMQA doc for review

Hi all,
Made edits as per my notes from today that reflect updated script language in both clean/tracked versions for your review and input.
Prefer to keep changes off eapps until we're closer to a final that's ready for MLB/MO, if ok with you.
Second reading notes also updated in eapps.

Kirsten Youngs, MAIIC (she/her/hers) | Communications Director
Ministry of Citizens' Services | Government Communications & Public Engagement
T: (250) 356-0543 | C: (250) 858-0555
I acknowledge and respect that I live and work on the traditional territory of the Lekwungen peoples, known today as the Esquimalt and Songhees Nations.

RE: For binder: OIPC summary - UPDATED

From: Leppard, Brianna CITZ:EX <Brianna.Leppard@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 14, 2021 12:03:47 PM PDT

Thanks Kass – I have updated MLB's calendar.
Brianna

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 14, 2021 11:55 AM
To: Leppard, Brianna CITZ:EX <Brianna.Leppard@gov.bc.ca>
Cc: Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Subject: FW: For binder: OIPC summary - UPDATED
This updated version has been emailed to MLB – but needs to be updated in her calendar.
Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Sent: October 14, 2021 11:51 AM
To: Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>; Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Cc: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>; Desaulnier, Vicki CITZ:EX <Vicki.Desaulnier@gov.bc.ca>; Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>; Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>
Subject: For binder: OIPC summary - UPDATED
Hi again, one more updated doc ahead of 2pm. This reflects requested descriptions from Kerry's team and GCPE edits in response.
Sam, is it possible for you to send out the recent versions pkg to everyone who is attending the 2pm – whatever MLB has in her binder?
Lots of versions going around 😊
Kirsten Youngs, MAIIC (she/her/hers) | Communications Director
Ministry of Citizens' Services | Government Communications & Public Engagement
T: (250) 356-0543 | C: (250) 858-0555
I acknowledge and respect that I live and work on the traditional territory of the Lekwungen peoples, known today as the Esquimalt and Songhees Nations.

FOR APPROVAL — Fwd: TB Sub - FOIPPA

From:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To:	Beare, Lisa CITZ:EX
Sent:	October 15, 2021 8:47:22 AM PDT
Attachments:	TB SUB FOIPPA Application Fee FIP - For Minister Approval.docx

For your approval.

Page 359 of 513 to/à Page 369 of 513

Withheld pursuant to/removed as

s.12

Page 370 of 513 to/à Page 371 of 513

Withheld pursuant to/removed as

s.12 ; s.14

Page 372 of 513 to/à Page 378 of 513

Withheld pursuant to/removed as

s.12

Re: FOR APPROVAL — Fwd: TB Sub - FOIPPA

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To: Beare, Lisa CITZ:EX
Sent: October 15, 2021 9:04:46 AM PDT

MLB approved. Jeannette will put the esig. Can you grab the eapp and send back to her?

Sent from my iPhone

> On Oct 15, 2021, at 8:47 AM, Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca> wrote:
>
> For your approval.
>
> <TB SUB FOIPPA Application Fee FIP - For Minister Approval.docx>

Re: FOR APPROVAL -- MLB SN - FOIPPA OIPC Mtg - 2021-10-15v2

From: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX
Sent: October 15, 2021 9:57:03 AM PDT

Approved

Honourable Lisa Beare, Minister
Ministry of Citizens' Services
250-356-8247

> On Oct 15, 2021, at 9:54 AM, Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca> wrote:
>
> Hi Minister
> SN for approval attached for your phone call with the Privacy Commissioner at 11am. All recent correspondence also attached – as well as summary table of concerns.
> Cheers
> Kass
> **Kassandra Lawal**
> Office 778-974-6009 | Cell 778-678-3776
> kassandra.lawal@gov.bc.ca
> <MLB SN - FOIPPA OIPC Mtg - 2021-10-15v2.docx>
> <Summary of OIPC concerns - Oct 13 2021v2.docx>
> <2021-10-13 Minister Beare Letter to OIPC.pdf>
> <2021-10-04 OIPC Letter to Minister Beare.pdf>
> <2021-08-11 ADM Pridmore Letter to OIPC.pdf>
> <2021-05-14 OIPC Letter to ADM Pridmore.pdf>

RE: FOI - Kass - August 2021 Calendar

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To: McEwen, Shaylene CITZ:EX
Sent: October 15, 2021 10:14:31 AM PDT

My harms have been marked on the FOI and is in my KL edits folder. Please return for IAO review, and then back to me for final sign off.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: McEwen, Shaylene CITZ:EX <Shaylene.McEwen@gov.bc.ca>
Sent: October 14, 2021 12:50 PM
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Subject: FOI - Kass - August 2021 Calendar

Hi Kass,

Your August 2021 Calendar has been redlined by the IAO and returned for review/approval.
Z:\5. SMA - FINAL SIGN-OFFs\Calendar - Kassandra Lawal - August 2021 (for review and approval) Redline CTZ-2021-14118 (IAO Redline)

Thank you,
Shay

QP binder -- FOI Statistics - Oct5.xlsx

From:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To:	McEwen, Shaylene CITZ:EX
Sent:	October 15, 2021 2:39:44 PM PDT
Attachments:	FOI Statistics - Oct5.xlsx

Shay – can you print, please and tuck in the front pocket of MLB's QP binder?
Thanks
Kass

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

FYI -- FOI Statistics - Oct5.xlsx

From:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To:	Beare, Lisa CITZ:EX
Sent:	October 15, 2021 2:41:08 PM PDT
Attachments:	FOI Statistics - Oct5.xlsx

This will be printed and tucked in the front pocket of your QP binder.
Cheers
Kass

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

FOR REVIEW -- 115954 - MIN IBN - DR Reg

From:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To:	Beare, Lisa CITZ:EX
Sent:	October 15, 2021 3:16:31 PM PDT
Attachments:	115954 - MIN IBN - DR Reg .docx

HI Minister
Fr your review – info note attached re Personal Information Disclosure for Storage Outside of Canada Regulation.
Cheers
Kass

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

BRITISH COLUMBIA | Ministry of Citizens' Services

INFORMATION NOTE
Advice to Minister Beare

Date: October 14, 2021 **CLIFF#:** 115954

ISSUE: The Personal Information Disclosure for Storage Outside of Canada Regulation

BACKGROUND:

With respect to disclosing personal information outside of Canada, B.C. currently has the strictest laws in the country. The *Freedom of Information and Protection of Privacy Act's* (the Act's) data-residency provisions restrict the B.C. public sector's ability to use many modern communications and collaboration tools, software and other technology. The Act mandates "blanket" data-residency protection for all personal information; however, that level of protection is not commensurate with the risk.

In October 2019, targeted amendments to the Act were passed to enable features associated with Canadian-based cloud technology. These amendments permit disclosure of personal information for temporary processing and disclosure and storage of metadata outside of Canada, but place conditions on the disclosures to ensure privacy is protected. However, feedback from public bodies covered by the Act indicated that the amendments were insufficient for enabling digital modernization.

s.12; s.13

s.12; s.13 Proposed amendments, expected to be enacted in Fall 2021, will repeal and replace the Act's data-residency provisions and introduce a new regulation-making authority, enabling the Minister to prescribe requirements related to disclosing personal information outside of Canada.

DISCUSSION:

s.13

s.13

CONCLUSION:

s.13

Contact: Kerry Pridmore, ADM
Appendix: s.13

115954 - MIN IBN - DR Reg

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To: Scott, Samantha CITZ:EX
Sent: October 15, 2021 3:17:17 PM PDT
Attachments: 115954 - MIN IBN - DR Reg .docx

FYI

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

FYI: scrum transcript

From:	Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Cc:	Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>, Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>, Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>, Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>, Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>, Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>
Sent:	October 18, 2021 3:11:30 PM PDT

Rough scrum transcript:

Q1 Rob Shaw, CHEK

Explain rationale behind modest fee? How much and why?

A: We believe people deserve access information in a timely manner

Modest application fee for non-personal requests

This is between $5-50 for other jurisdictions across Canada and I'm recommending right in the middle of that range.

Q2 Shaw follow-up

Is the fee meant to discourage people from making requests, like a barrier to information?

A: Not at all, it's modest and in line with other jurisdictions

Most requestors, about 98%, request 5 or less each year.

Personal requestors will continue to pay no fee at all.

Q3 Lisa Cordasco, Vancouver Sun

Last year, OIPC released report saying timeline responses are not in line with legislation, is govt ignoring rules?

A: I believe people should have timely access to FOI

And we've improved, govt's response rate was 76% when we took govt

We improved that up to 86% in 2019/20.

It's 81% now.

These amendments will help provide info to people quicker.

Q4 Cordasco follow up

Why are you doing this? To follow up on Rob's q.

A: Our legislation is outdated, we haven't updated FOIPPA since 2011.

Other jurisdictions across Canada have fees between $5-$50 and I'm recommending a modest fees in between that range.

Personal info will continue to be free

Q5 Shannon Waters, BC Today

Inaudible… other jurisdictions have done it but nothing helps?

A: This is separate from other fees for broad or large requests

Other jurisdictions across Canada have fees between $5-$50 and I'm recommending a modest fees in between that range.

Q6 Les Leyne, Times Colonist

Re Data management, BC has said before that data is to be stored in BC or maybe it was Canada – what's the consensus. You seem to be abandoning that?

A: COVID has changed the world and how we live, work, access services.

People want to keep connecting with their doctors online or access educational tools online.

These innovations weren't permitted under previous legislation and we need to fix that.

We need to improve access, protect privacy and ensure people have timely access to information they deserve.

Q7 Leyne follow up

What made you decide to override the OIPC's recommendations?

A: We thank the Commissioner and his team for his work and advice.

We're hearing from others like universities that the legislation is out of date and not helping them be competitive.

We can do that and keep people's info safe.

Nothing in Minister Dix's scrum relating to FOIPPA/health data.

Kirsten Youngs, MAIIC (she/her/hers) | Communications Director

Ministry of Citizens' Services | Government Communications & Public Engagement

T: (250) 356-0543 | C: (250) 858-0555

I acknowledge and respect that I live and work on the traditional territory of the Lekwungen peoples, known today as the Esquimalt and Songhees Nations.

CITZ Media Request: The Tyee - FOIPPA amendments

From:	Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>, Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>
Cc:	Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>, Harris, Megan GCPE:EX <Megan.Harris@gov.bc.ca>, Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>, Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>, Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Sent:	October 18, 2021 4:02:40 PM PDT

Hi – Suggested response for a media request from Andrew MacLeod for your review.
Thank you,
Jeremy

Reporter

Andrew MacLeod, Reporter
The Tyee
amacleod@thetyee.ca
250-885-7662

Deadline ASAP

Request

In the scrum this afternoon, minister Beare said jurisdictions charge between $5 and $50 for an FOI application. Any idea which jurisdictions she was talking about?

Recommendation

On background:

- 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.
- Right now, B.C. receives more FOI requests annually than the three western provinces, combined.
- 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.

Re: FOR APPROVAL -- FW: CITZ Media Request: The Tyee - FOIPPA amendments

From: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX
Sent: October 18, 2021 4:55:08 PM PDT

Approved
Get Outlook for iOS
From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: Monday, October 18, 2021 4:51:32 PM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
Subject: FOR APPROVAL -- FW: CITZ Media Request: The Tyee - FOIPPA amendments
Hi Minister
Media response for your approval – edited:
Request
In the scrum this afternoon, minister Beare said jurisdictions charge between $5 and $50 for an FOI application. Any idea which jurisdictions she was talking about?

Recommendation
On background:

- 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.
- Right now, B.C. receives more FOI requests annually than the other three western provinces, combined.
- Government processes more than 10,000 freedom of information requests each year and the average cost s.13 of processing a single FOI request is $3,000, though some large, complex requests can exceed this.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>
Sent: October 18, 2021 4:03 PM
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>; Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>
Cc: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Harris, Megan GCPE:EX <Megan.Harris@gov.bc.ca>; Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>; Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Subject: CITZ Media Request: The Tyee - FOIPPA amendments
Hi – Suggested response for a media request from Andrew MacLeod for your review.
Thank you,
Jeremy
Reporter
Andrew MacLeod, Reporter
The Tyee
amacleod@thetyee.ca
250-885-7662

Deadline ASAP

Request
In the scrum this afternoon, minister Beare said jurisdictions charge between $5 and $50 for an FOI application. Any idea which jurisdictions she was talking about?

Recommendation

On background:

- 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.
- Right now, B.C. receives more FOI requests annually than the three western provinces, combined.
- 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.

Re: FOR APPROVAL -- FW: CITZ Media Request: CTV News - FOIPPA amendments

From: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX
Sent: October 18, 2021 4:55:34 PM PDT

Yes this is better. Approved
Get Outlook for iOS
From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: Monday, October 18, 2021 4:53:30 PM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
Subject: FOR APPROVAL -- FW: CITZ Media Request: CTV News - FOIPPA amendments
Hi Minister
Media response for your approval , edited:
Recommendation
On background:

- Other jurisdictions charge anywhere from $5-$50. A modest fee in the middle of that range is being recommended and will be determined through regulation soon.
- Adding a fee to non-personal FOI requests is in line with other jurisdictions across Canada. It isn't s.13 a barrier to information elsewhere and it won't be here in B.C.
- The fee will apply to only those making non-personal requests. Nearly 98% of requestors make fewer than five requests a year.
- Those asking for personal information will not pay a fee at all.
- Right now, B.C. receives more FOI requests annually than the other three western provinces, combined.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca
Reporter
Penny Daflos, Reporter
CTV News (BC)
penny.daflos@bellmedia.ca
604-787-1871

Deadline ASAP

Request
Can you confirm Rob Shaw's reporting that the "modest applications fee" for FOI requests will be $25 and whether it'll apply to journalists?

Recommendation

On background:

- Other jurisdictions charge anywhere from $5-$50. A modest fee in the middle of that range is being recommended and will be determined through regulation soon.
- Adding a fee to non-personal FOI requests is in line with other jurisdictions across Canada. It isn't s.13 a barrier to information elsewhere and it won't be here in B.C.
- The fee will apply to only those making non-personal requests. Nearly 98% of requestors make fewer than five requests a year.
- Those asking for personal information will not pay a fee at all.
- Right now, B.C. receives more FOI requests annually than the other three western provinces, combined.

RE: CITZ Media Request: The Tyee - FOIPPA amendments

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
To: Olson, Michael GCPE:EX, Pridmore, Kerry CITZ:EX, Uppenborn, Jeremy GCPE:EX, Scott, Samantha CITZ:EX
Cc: Brouwer, Shauna CITZ:EX, Harris, Megan GCPE:EX, Williams, Susan GCPE:EX, Youngs, Kirsten R GCPE:EX
Sent: October 18, 2021 5:06:47 PM PDT

Approved with Michael's edits.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>
Sent: October 18, 2021 4:37 PM
To: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>; Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>; Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Cc: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Harris, Megan GCPE:EX <Megan.Harris@gov.bc.ca>; Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>; Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Subject: RE: CITZ Media Request: The Tyee - FOIPPA amendments
I have two suggestions in red below.

From: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Sent: October 18, 2021 4:27 PM
To: Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>; Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>; Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>
Cc: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Harris, Megan GCPE:EX <Megan.Harris@gov.bc.ca>; Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>; Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Subject: RE: CITZ Media Request: The Tyee - FOIPPA amendments
Matt and I support the below.
Do you want to point out Ontario charges for personals, only $5 but will leave with you if worth including.

From: Uppenborn, Jeremy GCPE:EX <Jeremy.Uppenborn@gov.bc.ca>
Sent: October 18, 2021 4:03 PM
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>; Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>
Cc: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Harris, Megan GCPE:EX <Megan.Harris@gov.bc.ca>; Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>; Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Subject: CITZ Media Request: The Tyee - FOIPPA amendments
Hi – Suggested response for a media request from Andrew MacLeod for your review.
Thank you,
Jeremy

Reporter

Andrew MacLeod, Reporter
The Tyee
amacleod@thetyee.ca
250-885-7662

Deadline ASAP

Request
In the scrum this afternoon, minister Beare said jurisdictions charge between $5 and $50 for an FOI application. Any idea which jurisdictions she was talking about?

Recommendation

On background:

- 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.
- Right now, B.C. receives more FOI requests annually than the other three western provinces, combined.
- Government processes more than 10,000 freedom of information requests each year and the average cost s.13 of processing a single FOI request is $3,000, though some large, complex requests can exceed this.

FYI: Validator release

From:	Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>, Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>
Cc:	Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>
Sent:	October 19, 2021 8:23:39 AM PDT
Attachments:	Social - HubSpot.jpeg

FYI

This is going out late this morning after 11 – great news from Freshworks!

Posting from: **FreshWorks Studio** | When: Oct

There was a major announcement in BC yesterday that we

BC has proposed amendments to its FOIPPA (Freedom of
Privacy Act) which includes updates to BC's data residenc
and businesses across BC, this opens up many possibilitie
streamlined & accessible services while offering even grea
information.

As a result, public bodies - and organizations like ours tha
greater access to modern tools and robust cloud-based te
providers like Amazon, Microsoft and Google. Lisa Beare,
summarized it well: "We're making changes today to keep
technology and provide the level of service that people exp

Our team regularly partners with public bodies in BC to de
the many digital modernization projects that are underway
modernization champions like our Minister Lisa Beare and
Information Officer, changes like these will continue to help
objectives set out in the province's digital framework.

We fully support this and are VERY excited to now have gr
move forward BC's vision for the future of digital governme
you should be too.

Posting from: **FreshWorks Studio** | When: Oct 19, 2021 11:02 AM PDT

There was a major announcement in BC yesterday that we wanted to share with you.

BC has proposed amendments to its FOIPPA (Freedom of Information and Protection of Privacy Act) which includes updates to BC's data residency requirements. For individuals and businesses across BC, this opens up many possibilities for faster and more streamlined & accessible services while offering even greater protection of personal information.

As a result, public bodies - and organizations like ours that work with them - will now have greater access to modern tools and robust cloud-based technology from reliable service providers like Amazon, Microsoft and Google. Lisa Beare, Minister of Citizen Services summarized it well: "We're making changes today to keep pace with advancements in technology and provide the level of service that people expect in the digital era."

Our team regularly partners with public bodies in BC to develop new applications as part of the many digital modernization projects that are underway at any given time. Thanks to modernization champions like our Minister Lisa Beare and CJ Ritchie, Government Chief Information Officer, changes like these will continue to help our public sector pursue the objectives set out in the province's digital framework.

We fully support this and are VERY excited to now have greater flexibility as we help them move forward BC's vision for the future of digital government. And if you live or work in BC, you should be too.

https://news.gov.bc.ca/releases/2021CITZ0048-001990

#BCTech #DigitalTransformation #DigitalGovernment #GCDigital



Amendments strengthen access to information, protect people's privacy | BC Gov News

https://news.gov.bc.ca

RE: Security Controls

From: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>
Sent: October 19, 2021 8:36:32 AM PDT

Confirming I am working on a response

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 19, 2021 8:34 AM
To: Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Subject: Security Controls
Importance: High

Good morning CJ and Kerry
MLB is asking for bullets to take into QP this morning re security controls we have discussed before – what are the four and a short explanation of each. Can you provide asap?

1. Technical – encryption etc
2. Contractual – we stipulate terms
3. Administrative – we decide what data to send
4. ?

Thanks much
kass

Kassandra Lawal
Senior Ministerial Advisor
Honourable Lisa Beare – Minister of Citizens' Services
Room 151| Parliament Buildings, Victoria, BC | V8W 9V1
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

Re: Security Controls

From: Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Cc: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Sent: October 19, 2021 8:36:45 AM PDT

Yes we will get this done and send back

Sent from my iPhone
CJ Ritchie
Associate Deputy Minister and Government Chief Information Officer
Ministry of Citizens' Services

> On Oct 19, 2021, at 8:33 AM, Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca> wrote:
>
> Good morning CJ and Kerry
> MLB is asking for bullets to take into QP this morning re security controls we have discussed before – what are the four and a short explanation of each. Can you provide asap?
>
> 1. Technical – encryption etc
> 2. Contractual – we stipulate terms
> 3. Administrative – we decide what data to send
> 4. ?
>
> Thanks much
> kass
> **Kassandra Lawal**
> Senior Ministerial Advisor
> Honourable Lisa Beare – Minister of Citizens' Services
> Room 151| Parliament Buildings, Victoria, BC | V8W 9V1
> Office 778-974-6009 | Cell 778-678-3776
> kassandra.lawal@gov.bc.ca

FOR MO APPROVAL: CITZ Media Request: FOIPPA legislation

From:	Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Cc:	Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>, Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>, Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>, Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Sent:	October 19, 2021 9:59:54 AM PDT

Reporter

Jeremy Hainsworth, Reporter
Glacier Media Digital
jhainsworth@glaciermedia.ca
604-608-5189 c: 778-835-4303

Deadline ASAP

Request

Reporter is working on a follow-up article on Bill22 announced Monday. The premier in 2019 said he was looking at inclusion of both Legislature information and whistleblower protection in an amended FOIPPA. Why are they not there? What level of initial request fee is the government looking at?

Recommendation

- The Freedom of Information and Protection of Privacy Act (FOIPPA) covers the public organizations in B.C.
- As in all other Parliamentary governments, the Legislative Assembly is separate and distinct from government and is therefore not included in FOIPPA or in these new amendments.
- Questions related to the transparency of the Legislative Assembly and the reporting of concerns should be directed to the legislature itself.
- This is done through the Legislative Assembly Management Committee and the Legislative Assembly Management Committee Act.
- Acts in British Columbia that pertain to Legislative Assembly matters are under the purview of the Attorney General.

Fees

- Other jurisdictions charge anywhere from $5-$50. A modest fee in the middle of that range is being recommended and will be determined through regulation soon.
- Adding a fee to non-personal FOI requests is in line with other jurisdictions across Canada. It isn't a barrier to information elsewhere and it won't be here in B.C.
- The fee will apply to only those making non-personal requests. Nearly 98% of requestors make fewer than five requests a year.
- Those asking for personal information will not pay a fee at all.
- Right now, B.C. receives more FOI requests annually than the other three western provinces, combined.
- 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.

RE: QA on accountability/transparency

From: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Cc: Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Sent: October 19, 2021 10:03:52 AM PDT

And more plain languaged summary of the items we have added that increase transparency:

- 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
- Requiring transparency in reasons for severing proactively disclosed records
- Adding two new public bodies (BC Assoc of Chiefs of Police; BC Assoc. of Municipal Chiefs of Police).

From: Youngs, Kirsten R GCPE:EX
Sent: October 19, 2021 10:01 AM
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Cc: Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Subject: QA on accountability/transparency

Kerry/Matt are updating this QA from the technical QA doc, but if needed now I can print?:

General:

- 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've heard from thousands of people, organizations and public sector bodies that our current legislation isn't working for them.
- We are a government that's focused on transparency, that's why we've increased our proactive disclosures and have committed to updating FOIPPA.

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.

FOR MO APPROVAL: CITZ Media Request: FOIPPA legislation - frequent requests

From:	Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Cc:	Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>, Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>, Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>, Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>, Harris, Megan GCPE:EX <Megan.Harris@gov.bc.ca>
Sent:	October 19, 2021 12:01:39 PM PDT

Hi all…another request for your approval re: prolific FOI applicants. Recommended response below, taken from the KM/QA document, with the addition of the highlighted line from program

Reporter

Tom Fletcher, Reporter
Black Press Media
tfletcher@blackpress.ca
250-888-3438

Deadline ASAP

Request

Reporter looking for confirmation on the FOI numbers Rob Shaw made public about frequent filers of FOI requests. Wants to know if 397 requests in a single year is an accurate figure and for what year? Also, is 4,000 FOI requests from opposition accurate, and for what year?

Recommendation

s.13

CITZ Media Request: FOIPPA legislation - COVID ministerial order

From:	Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>, Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>
Cc:	Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>, Harris, Megan GCPE:EX <Megan.Harris@gov.bc.ca>, Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>, Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Sent:	October 19, 2021 1:31:05 PM PDT

Reporter

Les Leyne, Reporter
Times Colonist
lleyne@timescolonist.com
250-889-4138

Deadline ASAP

Request

Reporter wants to know what ministerial order the Minister is referring to when she says "... we've been able to do that, to date, through COVID, through ministerial order. So we're making those changes permanent in this legislation."

What ministerial order is the Minister referring to? Any idea of how those institutions responded to the ministerial order?

Recommendation

- On March 26, 2020, Anne Kang, then-Minister of Minister of Citizens' Services, approved a ministerial order under the Freedom of Information and Protection of Privacy Act (FOIPPA) to temporarily permit the use of vital software and technologies in the public sector that have proven useful in B.C.'s successful efforts to flatten the curve.

- On June 5, that order was extended until Dec. 31, 2021.

- More information on that order can be found here: https://news.gov.bc.ca/releases/2020CITZ0010-001019

RE: FOR APPROVAL -- FW: FOR MO APPROVAL: CITZ Media Request: FOIPPA legislation - frequent requests

From: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX
Sent: October 19, 2021 2:25:04 PM PDT

Approved

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 19, 2021 12:43 PM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
Subject: FOR APPROVAL -- FW: FOR MO APPROVAL: CITZ Media Request: FOIPPA legislation - frequent requests
Media response below for your approval.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

Reporter

Tom Fletcher, Reporter
Black Press Media
tfletcher@blackpress.ca
250-888-3438

Deadline ASAP

Request

Reporter looking for confirmation on the FOI numbers Rob Shaw made public about frequent filers of FOI requests. Wants to know if 397 requests in a single year is an accurate figure and for what year? Also, is 4,000 FOI requests from opposition accurate, and for what year?

Recommendation

s.13

RE: FOR APPROVAL -- FW: FOR MO APPROVAL: CITZ Media Request: FOIPPA legislation

From: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX
Sent: October 19, 2021 2:26:39 PM PDT

Approved

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 19, 2021 11:11 AM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
Subject: RE: FOR APPROVAL -- FW: FOR MO APPROVAL: CITZ Media Request: FOIPPA legislation
Further edit:
Recommendation
• The Freedom of Information and Protection of Privacy Act (FOIPPA) covers the public organizations in B.C.
• As in all other Parliamentary governments, the Legislative Assembly is separate and distinct from government and is therefore not included in FOIPPA or in these new amendments.
• Questions related to the transparency of the Legislative Assembly and the reporting of concerns should be directed to the legislature itself.
• This is done through the Legislative Assembly Management Committee and the Legislative Assembly Management Committee Act.
• Acts in British Columbia that pertain to Legislative Assembly matters are under the purview of the Attorney General.
Fees
• Other jurisdictions charge anywhere from $5-$50. A modest fee in the middle of that range is being recommended and will be determined through regulation soon.
• The fee will apply to only those making non-personal requests. Nearly 98% of requestors make fewer than five requests a year.
• Those asking for personal information will not pay a fee at all.
• As well, we've increased the number of public proactive disclosures that make government information available to everyone for free. Just last week, every Minister's estimates binder was proactively released in full.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Lawal, Kassandra CITZ:EX
Sent: October 19, 2021 10:56 AM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
Subject: FOR APPROVAL -- FW: FOR MO APPROVAL: CITZ Media Request: FOIPPA legislation

Hi Minister

Media response below for your review and approval, with edits.

Let me know if you wish further edits.

Cheers

Kass

Recommendation

- The Freedom of Information and Protection of Privacy Act (FOIPPA) covers the public organizations in B.C.
- As in all other Parliamentary governments, the Legislative Assembly is separate and distinct from government and is therefore not included in FOIPPA or in these new amendments.
- Questions related to the transparency of the Legislative Assembly and the reporting of concerns should be directed to the legislature itself.

- This is done through the Legislative Assembly Management Committee and the Legislative Assembly Management Committee Act.
- Acts in British Columbia that pertain to Legislative Assembly matters are under the purview of the Attorney General.

Fees

- Other jurisdictions charge anywhere from $5-$50. A modest fee in the middle of that range is being recommended and will be determined through regulation soon.

s.13

- The fee will apply to only those making non-personal requests. Nearly 98% of requestors make fewer than five requests a year.
- Those asking for personal information will not pay a fee at all.

s.13

- As well, we've increased the number of public proactive disclosures that make government information available to everyone for free.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>
Sent: October 19, 2021 10:00 AM
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Cc: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>; Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Subject: FOR MO APPROVAL: CITZ Media Request: FOIPPA legislation

Reporter

Jeremy Hainsworth, Reporter
Glacier Media Digital
jhainsworth@glaciermedia.ca
604-608-5189 c: 778-835-4303

Deadline ASAP

Request

Reporter is working on a follow-up article on Bill22 announced Monday. The premier in 2019 said he was looking at inclusion of both Legislature information and whistleblower protection in an amended FOIPPA. Why are they not there? What level of initial request fee is the government looking at?

Recommendation

- The Freedom of Information and Protection of Privacy Act (FOIPPA) covers the public organizations in B.C.
- As in all other Parliamentary governments, the Legislative Assembly is separate and distinct from government and is therefore not included in FOIPPA or in these new amendments.
- Questions related to the transparency of the Legislative Assembly and the reporting of concerns should be directed to the legislature itself.
- This is done through the Legislative Assembly Management Committee and the Legislative Assembly Management Committee Act.
- Acts in British Columbia that pertain to Legislative Assembly matters are under the purview of the Attorney General.

Fees

- Other jurisdictions charge anywhere from $5-$50. A modest fee in the middle of that range is being recommended and will be determined through regulation soon.

s.13

- The fee will apply to only those making non-personal requests. Nearly 98% of requestors make fewer than five requests a year.
- Those asking for personal information will not pay a fee at all.

s.13

Rolling List: CITZ Media Request: FOIPPA legislation

From: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 19, 2021 2:37:45 PM PDT

s.13

Reporter

Les Leyne, Reporter
Times Colonist
lleyne@timescolonist.com
250-889-4138

Deadline ASAP

Request

Reporter wants to know what ministerial order the Minister is referring to when she says "... we've been able to do that, to date, through COVID, through ministerial order. So we're making those changes permanent in this legislation."

What ministerial order is the Minister referring to? Any idea of how those institutions responded to the ministerial order?

Recommendation

- On March 26, 2020, Anne Kang, then-Minister of Minister of Citizens' Services, approved a ministerial order under the Freedom of Information and Protection of Privacy Act (FOIPPA) to temporarily permit the use of vital software and technologies in the public sector that have proven useful in B.C.'s successful efforts to flatten the curve. On June 5, that order was extended until Dec. 31, 2021.

- More information on that order can be found here: https://news.gov.bc.ca/releases/2020CITZ0010-001019

Consult Summary

From:	Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
To:	Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>, Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Cc:	Reed, Matt CITZ:EX <Matt.Reed@gov.bc.ca>
Sent:	October 19, 2021 3:31:22 PM PDT
Attachments:	Minister RT Post-Secondary Sector - High Level Summary - June 17, 2021.pdf, Public report on 2021 FOIPPA engagement - FINAL.pdf, Ipsos Privacy Survey - Draft Results Deck (Aug 6) (002).pdf, Minister RT Tech Sector - High Level Summary - June 8, 2021.pdf, govTogetherBC - FOIPPA Final Report - Aug 10, 2021.docx, Summary - Minister roundtable - Health sector 2021-06-02.pdf

Enclosed are all the reports in one, easy access email.
The final public report on pg. 26 lists all of who was spoken with.
Kerry

BRITISH COLUMBIA | Ministry of Citizens' Services

Summary of Discussion

FOIPPA Engagement - Post-secondary sector

June 17, 2021
4:00 – 5:00pm

BC Government Attendees:	*Ministry of Citizens' Services* Lisa Beare, Minister of Citizens' Services CJ Ritchie, Associate Deputy Minister Kerry Pridmore, ADM, Corporate Information and Records Management Matt Reed, ED, Strategic Policy & Legislation	*Ministry of Advanced Education & Skills Training* Anne Kang, Minister of Advanced Education and Skills Training Shannon Baskerville, Deputy Minister Kevin Brewster, ADM and EFO, Finance, Technology and Management Services Tony Loughran, ADM, Governance, Legislation and Corporate Planning
Post-Secondary Institution Attendees:	Blair Littler, VP, The Research Universities' Council of British Columbia Brett Fairbairn, President and Vice-Chancellor, Thompson Rivers University Dennis Johnson, President, College of New Caledonia Gail Murphy, VP, Research and Innovation, The University of British Columbia Hubert Lai, University Council, The University of British Columbia Ian Humphreys, VP, Administration and International Dev., Vancouver Community College Max Blouw, President, The Research Universities' Council of British Columbia Rajiv Jhangiani, Assoc. VP, Open Education, Kwantlen Polytechnic University Tom Roemer, VP, Education, Research and International, BC Institute of Technology Wency Lum, Chief Information Officer, University of Victoria	

Session purpose:

- Feedback on B.C.'s public sector privacy rules, specifically the current data residency requirements and opportunities for improvement.

Key themes:

- Data residency restrictions impacting competitiveness and increasing costs
  - Pandemic put pressure on institutions. Were able to meet needs of students and communities due to expanded technology options provided by Ministerial Order.
    - Temporary nature of Order cost institutions more as unable to sign multi-year contracts.
    - Institutions agree they want to continue accessing the tools moving forward.
  - Often industry standard tools are unavailable for student/faculty use due to data residency restrictions (e.g. nursing)
    - Non-standard and out of date tools are being used in classrooms as cannot use continually updated cloud-based versions
  - Smaller/rural institutions need the ability to access tools online – setting up local instances are cost prohibitive
  - Cyber security standards set by large corporations (outside Canada) often better than what institution can establish locally.
    - Data residency workarounds can be expensive and possibly less secure.

  - Need to future-proof any changes – technology changing at a rapid rate.
    - What is implemented today that meets data residency requirements, may not be in compliance tomorrow if they provider changes how data is managed.

- Privacy Impact Assessments time consuming
  - Faculty may avoid PIA process due to amount of work to complete. Possible solution is bringing someone in to complete but often costs more than the software.
  - PIA requirements impacting ability to keep up with research – need to enable researchers to collaborate quickly across Canada and the world (e.g. COVID research) without worrying about privacy concerns.



Information Access and Privacy

Stakeholder Consultation Overview

April – August 2021

BRITISH COLUMBIA | Ministry of Citizens' Services

Executive Summary

British Columbia's Freedom of Information and Protection of Privacy Act (FOIPPA) balances government's accountability to the public through access to information with a person's right to privacy.

The COVID-19 pandemic has shifted how government does business, with technology being used more than ever to provide safe and convenient services to people. The Ministry of Citizens' Services undertook engagement through spring and summer 2021 with a variety of stakeholders to understand how the pandemic and other shifts in society have impacted how people view government information access and privacy.

Through a combination of roundtable meetings and presentations to stakeholder groups, the ministry heard from representatives of the over 2,900 public bodies covered by FOIPPA on improvements that could be made to better support their operations while also maintaining government's commitment to increase access to information. In addition, public surveys were hosted to gain insight on how the public's perception of information access and protection of privacy may have changed since the last survey in 2018; especially in light of government expanding many services online in the last year.

Engagement and consultation focussed on two key themes:

- Service modernization
- Privacy enhancement

By gathering input from a wide range of individuals, businesses, Indigenous partners, and stakeholders, government will be well positioned to understand what is important to people as it considers ways to improve how people's information is protected while keeping the B.C. public sector accountable.



Background

The Freedom of Information and Protection of Privacy Act (FOIPPA) was introduced in 1993 and keeps government accountable to the public and protects the privacy of British Columbians.

British Columbia has long been a leader in Canada with respect to privacy protection and access to information; however, FOIPPA has fallen out of step with similar statutes in other jurisdictions. Apart from the minor amendments made in 2019, the Act has not been substantially updated since 2011. As a result, it has been outpaced by considerable advancements in technology, significant changes in the way people access government services and evolving privacy protection expectations.

The Ministry of Citizens' Services is looking at opportunities to:

- Enable service modernization across the public sector, which will allow government to provide better services to British Columbians.
- Enhance public-sector privacy protections.
- Demonstrate the Province's commitment to diversity, inclusion, reconciliation, and equity.

There are a large number of stakeholders who have an interest in FOIPPA, including the over 2,900 public bodies covered by the Act as well as professional associations, special interest groups, Indigenous partners, the Office of the Information and Privacy Commissioner (OIPC) and the public.

From 2017 to 2019, there was substantial engagement completed on the topic of information access and privacy to understand stakeholder concerns and priority issue identification. Feedback from these stakeholder sessions, as well as recommendations from Special Committees of the Legislative Assembly that reviewed FOIPPA, and the OIPC, has informed opportunities to improve the way people's information is protected while keeping the Province accountable. These opportunities were presented to stakeholders through recent consultation.



Consultation Overview

Building on the productive 2017-2019 consultations, the ministry re-engaged with many of the same stakeholder groups to confirm their previous input and present policy options based on their feedback – including gaining an understanding of potential organizational impacts from the changes. Engagement was undertaken between April and August 2021 with B.C broader public sector bodies, government ministries, Indigenous partners, the technology sector, and the general public.

Public sector feedback was received through roundtable meetings and presentations to representatives in key sectors of the broader public sector (such as post-secondary institutions, crown corporations and health authorities) as well as government ministries.

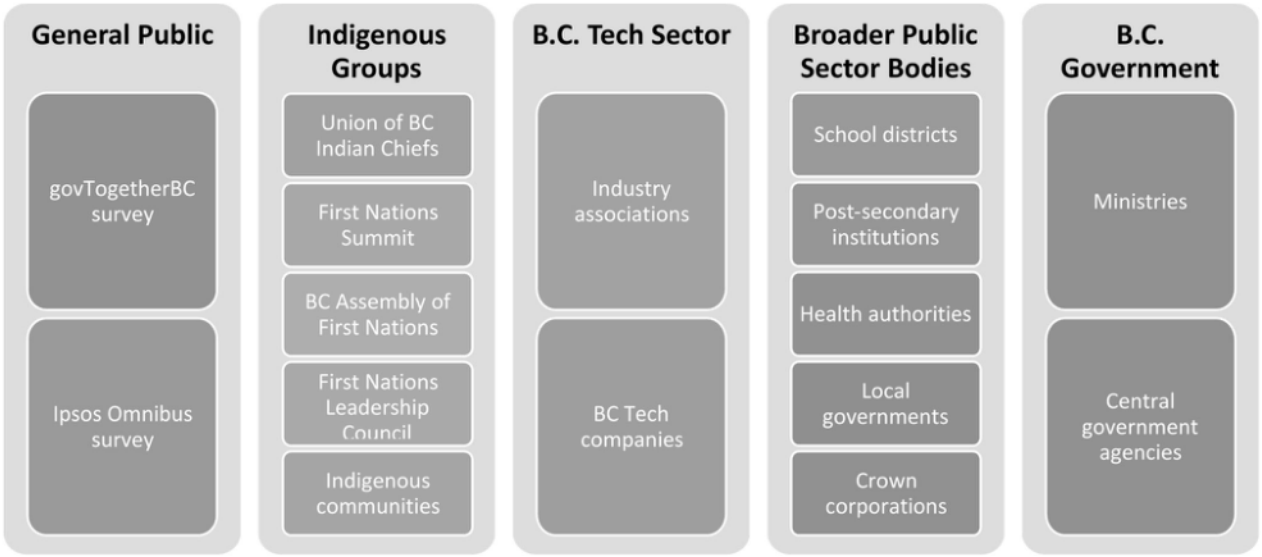
For the general public, a survey was hosted on govTogetherBC which followed-up on a similar survey from spring 2018. The purpose of the survey was to understand if people's thoughts on access to government information and the protection of privacy has changed since that time – especially with the expansion of many government services online during the pandemic. The questions focused on how individuals access government information, data protection, the Freedom of Information (FOI) process, reporting privacy breaches, and offences and penalties. Over 1,700 individuals responded to the survey between June 15 and July 15. [Survey content and results can be found in Appendix 1]

To ensure a broad representation of respondents, a similar survey was conducted by Ipsos Omnibus with 800 adult British Columbians throughout the province. [Survey content and results can be found in Appendix 2]

In addition, special focus was placed on engaging with Indigenous partners to better understand how reconciliation efforts can be supported through improving access to information and privacy rules. This work is still underway and has included meetings with Indigenous organizations, discussions with Treaty First Nations representatives as well as a questionnaire that was sent to over 200 First Nations leaders in communities throughout the province.

Summary of Participants

[See Appendix 3 for detail on sessions and participating organizations.]



| Findings

Theme 1: Service Modernization

Current state

British Columbians are very active when it comes to using the Freedom of Information (FOI) process – the B.C. government receives more FOI requests every year than most other jurisdictions in Canada. While many general FOI requests (requests that are not for an individuals' own personal information) ensure that high-value government information is shared with the public, others are overly broad and directed at multiple public bodies. These requests do not typically result in responsive records and as such, do not increase transparency. Responding to these broad requests impacts the capacity for public bodies to effectively serve all FOI applicants and has the potential to negatively impact day-to-day operations.

In 2004, FOIPPA was updated to keep British Columbians' personal information in Canada; however, these changes have prevented the B.C. public sector from using modern tools and new or innovative technology to provide services to British Columbians. It has been almost twenty years since these requirements were implemented, and people's expectations have changed. British Columbians expect more and better online

services from the public sector – especially during public emergencies such as the COVID-19 pandemic. As well, technology has also evolved considerably since 2004, with many enhancements to the ways personal data can be protected.

To ensure government can continue providing services during the pandemic, a ministerial order was issued to enable the use of online tools such as virtual classrooms, health services, voter registration and others. People see benefit to these digital tools and government is considering how to continue improving online tools and technologies to help people access public services in the future.

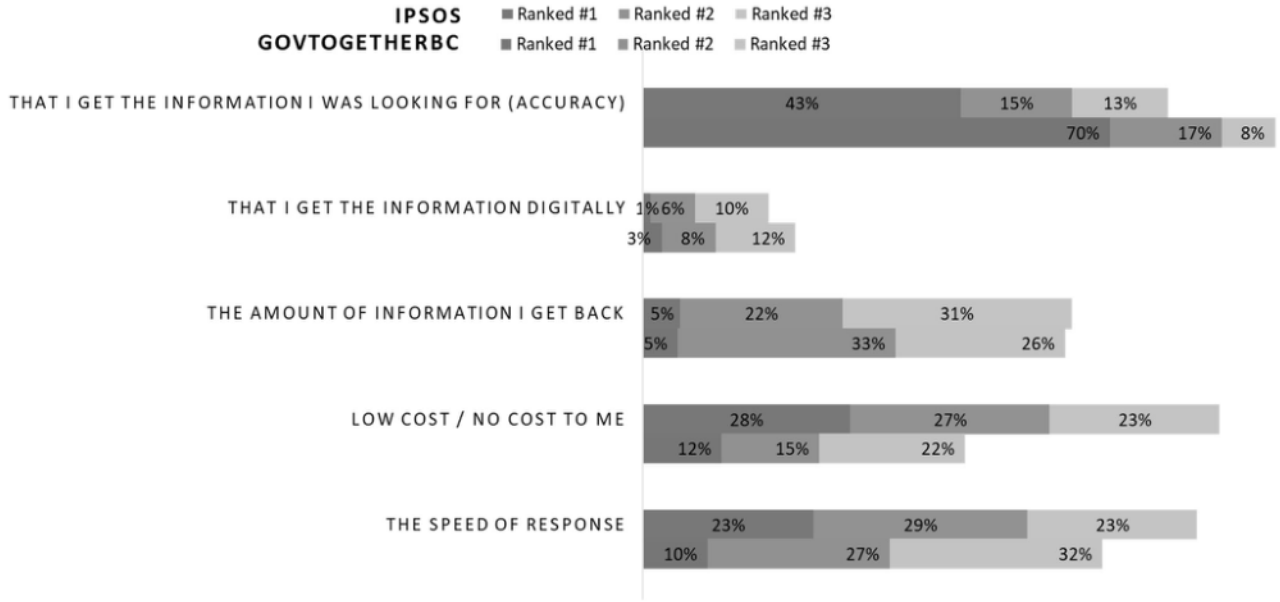
Response from stakeholders

Through consultations with public bodies, the ministry learned that the impact of increased FOI requests in the past several years have been felt across the public sector. In the health sector, there has been a substantial increase of general requests during the COVID-19 pandemic which is straining the capacity of an already busy health care system. Staff of local governments are balancing the day-to-day functions of running a municipality with responding to an increasing number of FOI requests, which is causing significant operational challenges. Discussions focussed on opportunities to improve the FOI process.

While 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 low/no cost and speed of response were secondary.

> *"If I am seeking information, the most important thing is that the information is accurate. There's no point in low cost or speed if I cannot rely on that information."*
>
> - Information Access and Privacy survey respondent

Figure 1 – How would you rank these in order of importance when seeking government information or data (i.e. not your own information)?

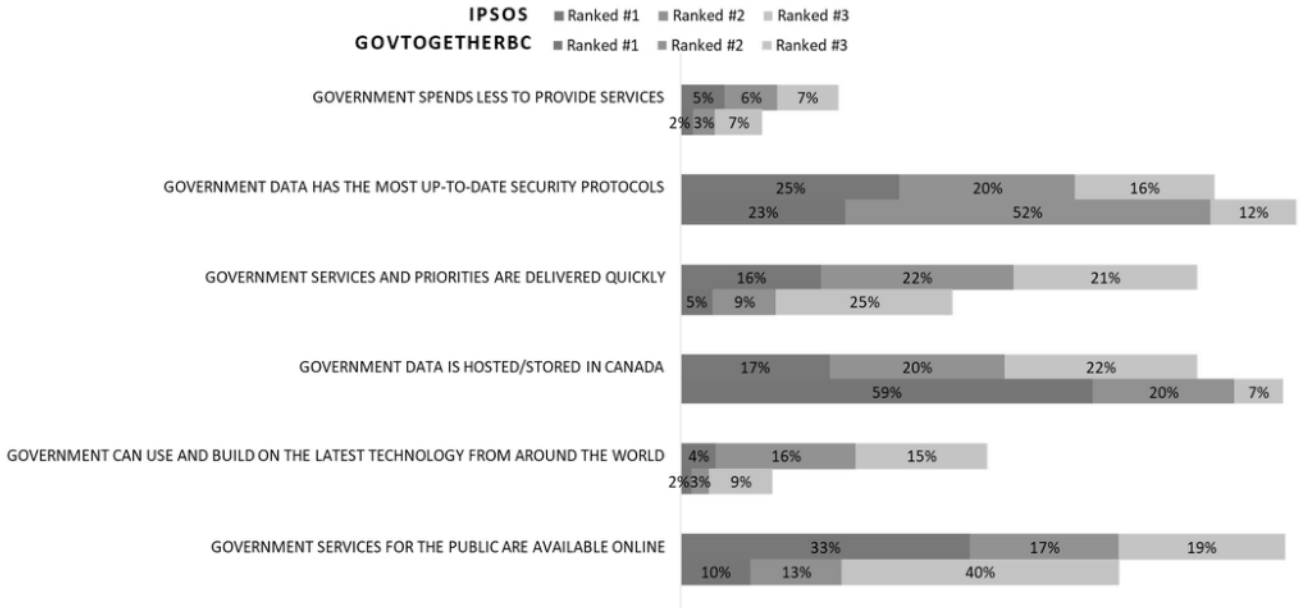


When discussing B.C.'s current requirements to keep British Columbians' personal information in Canada, most public bodies agreed that the current restrictions are slowing their ability to: provide necessary services to British Columbians, be innovative, collaborate with other jurisdictions, and compete in a world market. Health sector participants highlighted examples where cross-country and worldwide collaboration during COVID were impacted by the current restrictions. In the post-secondary sector, non-standard and out-of-date tools are being used in classrooms as instructors are unable to use the most effective tools available, which is negatively impacting post-secondary institution competitiveness. Smaller and rural organizations also highlighted a number of tools that are currently unavailable due to the restrictions and noted that developing alternatives can be cost prohibitive.

Similarly, during discussions with the B.C. tech sector, it was highlighted that being able to access modern technology (e.g., cloud computing) to support the public sector would improve service delivery. Sector representatives also noted that it would increase the competitiveness of small tech businesses by enabling them to use faster, more powerful, and often more economical international cloud technology when working with government.

While survey respondents were divided on whether or not the storage of personal information inside of Canada was important to them, there was a general consensus that government needs to be able to provide quality modernized services to citizens and needs to ensure that B.C.'s information is kept safe and secure.

Figure 2 – When thinking about accessing government services and information, what is most important to you?



> *"Data security is paramount. I trust government to ensure our most-sensitive data is being handled using world-leading information security best practices. This must be balanced with the need to provide services to the public promptly and accessibly which demands an approach to information security that scales with the potential damage of the information being improperly accessed."*
>
> *"Data is important and needs to be protected from bad actors. It would be preferable that Canadian data stays in Canada."*
>
> - Information Access and Privacy survey respondents

Theme 2: Privacy Enhancement

Current state

The B.C. public sector has one of the most rigorous privacy regimes in all of Canada. Protecting the privacy of British Columbians is a top priority for government and broader public sector bodies. As stated above, British Columbians' expectations of privacy are ever evolving. The Province is committed to continuously improving its privacy framework in response to these expectations with input from stakeholders.

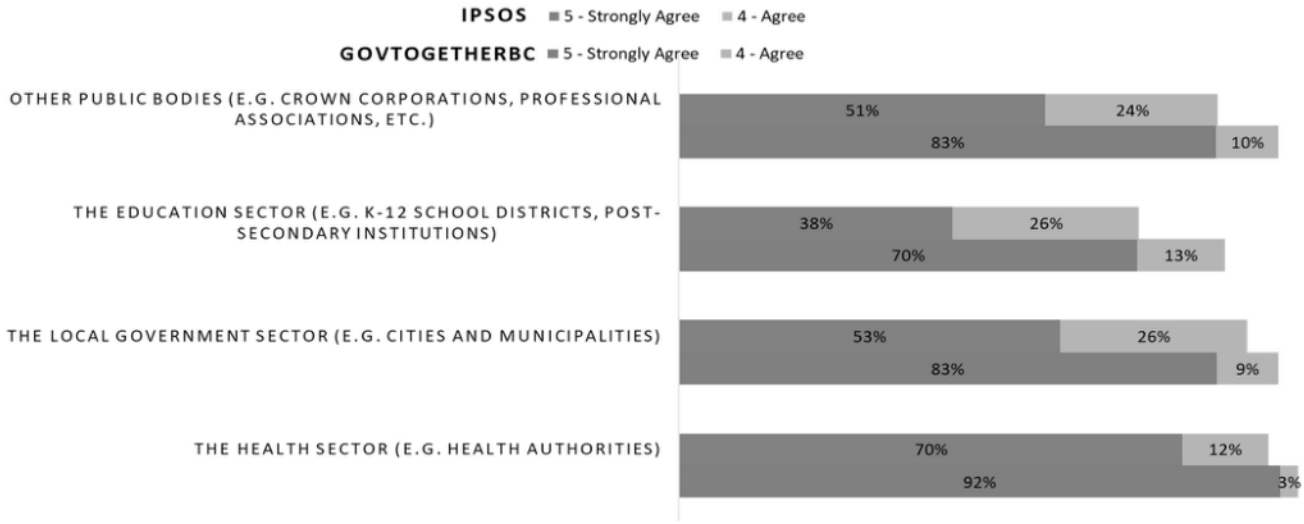
Response from stakeholders

Discussions with stakeholders focussed on opportunities to ensure B.C. remains at the forefront of privacy protection in Canada and all participants agreed that protecting the privacy of British Columbians is imperative.

In discussions with broader public sector bodies, all sectors acknowledged that while privacy-enhanced practices— such as reporting privacy breaches, conducting privacy impact assessments (PIAs), and having a framework in place to manage privacy—can often be time consuming, they are vital. Smaller public bodies have limited capacity, and participants highlighted the need for any privacy protections to be proportionate to the sensitivity of the personal information held, while also providing appropriate supports and training.

Participants in the govTogetherBC public survey and Ipsos Omnibus survey strongly indicated that they agree that broader public sector bodies should notify the affected person or the OIPC if their private information was breached. Below is a comparison of responses across both surveys.

Figure 3 – How strongly do you feel the following public bodies should be legally required to notify you and/or the Office of the Information and Privacy Commissioner if your private information is breached?

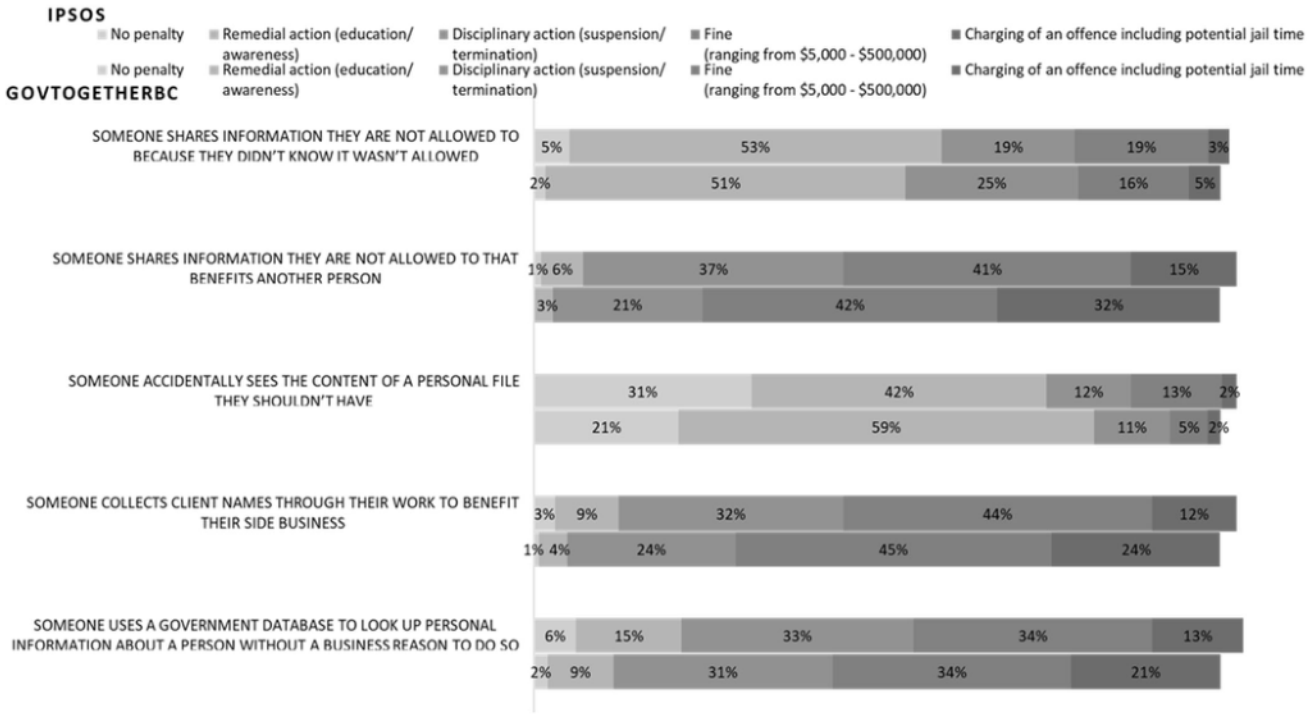


Written comments in both surveys had a common theme of "security and privacy". Respondents made it clear that ensuring that personal information is secure is critical. Several respondents noted that government should be held to higher data protection standards compared to other organizations and should have increased security protections in place to protect people's personal information.

Additionally, respondents emphasized the consequences of privacy breaches and called for a strengthening of laws relating to privacy and security. Many comments also stressed the increasing significance of personal data as the world becomes more digital.

> *"When accessing government services, people are required to provide personal information. I believe it is of utmost importance that the citizens of BC can trust that their personal information will not be compromised."*
>
> - Information Access and Privacy survey respondent

Figure 4 – For each of the scenarios below, which penalty seems most appropriate for the offence?



Conclusion

It is clear from stakeholder feedback that individuals, businesses, and public bodies in British Columbia are interested and engaged on how the Province enables transparency through access to information and protects privacy. This summary provides a snapshot of major items raised during the recent discussions and surveys on privacy and access. All feedback received will inform next steps as the ministry reviews FOIPPA.



Appendix 1: govTogetherBC survey content and results

Minister's Welcome

In Spring 2018, we asked for your ideas to improve the rules that govern both access to information and the protection of your personal information. A summary of the results can be found here.

We recognize a lot has changed since those discussions took place. The COVID-19 pandemic has shifted how government does business, with technology being used more than ever to provide safe and convenient services to people.

The Ministry of Citizens' Services wants your thoughts on access to government information and the protection of privacy. Your input will help us improve our services in the future. Thank you for taking part!

Hon. Lisa Beare
Minister of Citizens' Services

Section 1 – Accessing government information

1. Currently, what is your primary source for information from government?
   - 43.39% Government websites
   - 11.37% Newspapers
   - 6.38% Government social media channels (e.g., Facebook, Instagram, Twitter etc.)
   - 10.08% Other social media channels (e.g., Facebook, Instagram, Twitter etc.)
   - 11.65% TV
   - 16.63% Other

2. Has where you get government information changed during the pandemic?
   - 14.50% Yes
   - 84.66% No

2b. If yes, how?

[Written responses not shown to protect the privacy of respondents]

3. In the past year, which of the following have you accessed or used?
    - 55.82% Virtual doctor's appointment
    - 20.88% Video conferencing with government staff (e.g., Zoom, MS Teams, GoToMeeting, etc.)
    - 23.85% BC Services Card mobile app
    - 11.42% Virtual Schools (e.g., K-12, post-secondary)
    - 75.25% Booking an appointment online for government services (e.g., COVID vaccination, ICBC)
    - 46.98% Online laboratory test results
    - 49.55% Paying government bills online
    - 37.79% Applying for COVID-19 benefits or supports
    - 42.39% Online voter registration and/or vote-by-mail package request (Elections BC)

Section 2 – Data residency

In 2004, the Freedom of Information and Protection of Privacy Act (FOIPPA) was updated to keep British Columbians' personal information in Canada; however, these rules have left B.C. falling behind other provinces. It has also made it more difficult and often more expensive for government to use new or innovative technology.

It's been almost 20 years since these requirements were implemented. Since then, there have been big advances in technology and information security. People's expectations have also changed; they expect more and better online services from their governments today than ever before – especially during the pandemic.

To ensure government can continue providing services during the pandemic, a ministerial order was issued to enable the use of online tools such as virtual classrooms, online health services, voter registration and others. People have told us they see benefit to these digital tools and government is considering how these new and innovative technologies can help people to access services in the future.

4. When thinking about accessing government services and information, what is most important to you?
    - 9.96% Government services for the public are available online
    - 1.53% Government can use and build on the latest technology from around the world
    - 58.80% Government data is hosted/stored in Canada

4.53% Government services and priorities are delivered quickly
23.49% Government data has the most up-to-date security protocols
1.70% Government spends less to provide services

5. Provide some detail why the option(s) you chose in the previous question are so important.

   [Written responses not shown to protect the privacy of respondents]

6. How concerned are you about the following information security risks?
   - 31.41% Hackers stealing my personal information and/or committing identity theft
   - 27.57% Government using my personal information in ways I have not consented
   - 11.58% Organizations selling my personal information
   - 1.53% Accidental information loss, such as misdirected mail
   - 27.91% Unauthorized monitoring by other governments

7. When it comes to security, the more sensitive a piece of information or data is, the more strongly we should protect it. Reflecting on what is most important to you, how would you rank the sensitivity of the following personal information or data types?
   - 34.79% Health (e.g., lab results, immunization history, prescriptions)
   - 46.90% Financial (e.g., student loan balances, social insurance number, personal tax history)
   - 1.02% Employment / business (e.g., employment history, business permits, contracts)
   - 0.06% Education (e.g., GPA, exam results, evaluations from instructors)
   - 0.91% Natural resources (e.g., land use permits, water rights applications, hunting/fishing licenses)
   - 5.57% Personal demographics (e.g., gender, race, religion)
   - 4.21% Justice (e.g., court documents, offences)
   - 6.54% Social services (e.g., child protection records, income assistance, child support information)

Section 3 – The FOI Process

The Freedom of Information and Protection of Privacy Act (FOIPPA) makes public bodies more accountable by giving you the right to access most government records as well as giving individuals a right of access to, and a right to request correction of personal information about themselves. For more information about the Freedom of Information

request process, please see https://www2.gov.bc.ca/gov/content/governments/about-the-bc-government/open-government/open-information/freedom-of-information.

Government is very committed to providing this service; however, requests for government information (e.g. reports, emails, audits, etc.) costs government an average of $3,000 to process each request and only about $5 per request is recouped through fees. There is currently no fee to make an application, but you can be charged for time preparing information, making copies, for shipping, etc.

8. Which (if any) freedom of information (FOI) requests have you made?

   I have made a request for:
   - 14.84% My own information
   - 10.30% Other government information
   - 78.61% None of the above

9. How would you rank these in order of importance when seeking government information or data (i.e. not your own information)?
   - 9.69% The speed of response
   - 11.85% Low cost / no cost to me
   - 5.19% The amount of information I get back
   - 2.79% That I get the information digitally
   - 70.48% That I get the information I was looking for (accuracy)

10. Provide some detail why the option(s) you chose in the previous question are so important.

    [Written responses not shown to protect the privacy of respondents]

Section 4 – Reporting privacy breaches

Government holds a lot of information about British Columbians. While every reasonable effort is taken to keep your personal information safe and secure, privacy breaches do happen.

A privacy breach occurs when personal information is accidentally or deliberately accessed, used, or shared in a way that is not authorized by the Freedom of Information and Protection of Privacy Act (FOIPPA). If a privacy breach does occur in a government ministry, a formal breach management process is followed to ensure that the breach is quickly contained and resolved to minimize the impact as much as possible.

While many of the 2,900 public bodies covered by FOIPPA such as Crown corporations, universities, health authorities and municipalities have a similar process in place, they have no legal requirement to report privacy breaches to the Information and Privacy Commissioner or notify affected individuals.

11. How strongly do you feel the following public bodies should be legally required to notify you and/or the Office of the Information and Privacy Commissioner if your private information is breached?

	1 – Strongly Disagree	2	3	4	5 – Strongly Agree	Prefer not to answer
The health sector (e.g. health authorities)	3.30%	0.06%	0.62%	2.69%	92.44%	0.39%
The education sector (e.g. K-12 school districts and post-secondary institutions)	2.58%	2.02%	9.07%	13.49%	70.44%	1.62%
The local government sector (e.g. cities and municipalities)	2.80%	1.01%	2.97%	9.41%	82.70%	0.62%
Other public bodies (e.g. Crown corporations, professional associations, etc.)	2.97%	0.67%	3.02%	9.63%	82.59%	0.45%

Section 5 – Offences and penalties

There are penalties in place to deter anyone from breaking the access and privacy laws set out in FOIPPA. Currently, a person who misleads an Office of the Information and Privacy Commissioner investigation can be fined up to $5,000, while any individual committing a privacy protection offence could be fined up to $2,000. Service providers who break these rules can be fined up to $25,000 and corporations can face penalties of up to $500,000.

Recognizing not all offenses are worthy of large fines, government is looking at alternative penalties for FOIPPA offences.

12. For each of the scenarios below, which penalty seems most appropriate for the offense? Note: Severity of penalty increases from left to right.

	No penalty	Remedial action (education/ awareness)	Disciplinary action (suspension/ termination)	Fines less than $5,000	Fines up to $5,001 and $50,000	Fines up to $50,001 and $500,000	Charging of an offence including potential jail time
Someone uses a government database to look up personal information about a celebrity, neighbour, or family member without a business reason to do so	1.96%	9.35%	31.19%	9.97%	15.90%	8.12%	21.28%
Someone collects client names through their work to benefit their side business	0.73%	3.98%	23.96%	7.17%	24.52%	13.38%	23.96%
Someone accidentally sees the content of a personal file they shouldn't have	20.55%	59.18%	10.86%	2.30%	2.13%	0.95%	1.79%

Someone shares information they are not allowed to that benefits another person	0.11%	2.52%	21.33%	9.46%	21.00%	11.53%	31.69%
Someone shares information they are not allowed to because they didn't know it wasn't allowed.	1.62%	51.29%	24.58%	7.05%	6.16%	2.52%	4.54%

Section 6 – General

If you have any further comments about access to government information and protection of privacy, please let us know below.

[Written responses not shown to protect the privacy of respondents]

Section 7 – Tell us about yourself

To get a better understanding about who is responding to this questionnaire, please provide a bit of detail about yourself. These questions, like the other questions in this questionnaire, are optional.

13. What best describes how you are responding to this questionnaire? I am responding as a:

    2.07% Representative of a commercial or non-profit organization
    89.08% Interested member of the public
    2.35% Representative from a local government
    0.11% Representative of an Indigenous organization
    0.11% Representative of a First Nations government
    4.70% Other

14. Which region of the province do you reside in?

36.62%	Vancouver Island / Coast
44.57%	Mainland / Southwest
8.96%	Thompson / Okanagan
3.36%	Kootenay
1.51%	Cariboo
1.01%	North Coast
1.12%	Nechako
0.78%	Northeast
0.22%	I live outside of B.C.

Appendix 2: Ipsos survey results

1. In which of the following B.C. regions do you live?
   - 53% Greater (Metro) Vancouver
   - 17% Vancouver Island
   - 30% Somewhere else (North, Interior, Okanagan, Fraser Valley, Kootenays, etc.)

2. In the past year, which of the following have you accessed or used?
   - 63% Booking an appointment online for government services (e.g., COVID vaccination, ICBC)
   - 48% Virtual doctor's appointment
   - 35% Online laboratory test results
   - 35% Paying government bills online
   - 32% Applying for COVID-19 benefits or supports
   - 23% Online voter registration and/or vote-by-mail package request (Elections BC)
   - 22% BC Services Card mobile app
   - 14% Video conferencing with government staff (e.g., Zoom, MS Teams, GoToMeeting, etc.)
   - 13% Virtual Schools (e.g., K-12, post-secondary)
   - 9% None of these

3. When thinking about accessing government services and information, what is most important to you? Please rank the following elements from greatest to least importance.

   Top Rank % / Average Rank
   - 33% / 2.7 Government services for the public are available online
   - 25% / 3.0 Government data has the most up-to-date security protocols
   - 17% / 3.2 Government data is hosted/stored in Canada
   - 16% / 3.1 Government services and priorities are delivered quickly
   - 4% / 4.1 Government can use and build on the latest technology from around the world
   - 5% / 4.9 Government spends less to provide services

4. How concerned are you about the following information security risks? Please rank the following elements from greatest concern to least concern.

   Top Rank % / Average Rank

   62% / 1.8 Hackers stealing my personal information and/or committing identity theft

   15% / 2.7 Government using my personal information in ways I have not consented

   12% / 3.0 Organizations selling my personal information

   8% / 3.6 Unauthorized monitoring by other governments

   4% / 3.9 Accidental information loss, such as misdirected mail

5. When it comes to security, the more sensitive a piece of information or data is, the more strongly we should protect it. Reflecting on what is most important to you, how would you rank the sensitivity of the following personal information or data types?

   Top Rank % / Average Rank

   49% / 2.2 Financial (e.g., student loan balances, social insurance number, personal tax history)

   28% / 2.7 Health (e.g., lab results, immunization history, prescriptions)

   9% / 4.6 Social services (e.g., child protection records, income aid, child support information)

   4% / 4.9 Justice (e.g., court documents, offences)

   3% / 4.4 Employment / business (e.g., employment history, business permits, contracts)

   3% / 5.5 Personal demographics (e.g., gender, race, religion)

   2% / 5.5 Education (e.g., GPA, exam results, evaluations from instructors)

   1% / 6.2 Natural resources (e.g., land use permits, water rights applications, hunting/fishing licenses)

6. Which (if any) freedom of information (FOI) requests have you made?

   14% I have made a request for my own information

   6% I have made a request for other government information

   82% None of the above

7. How would you rank these in order of importance when seeking government information or data (i.e., not your own information)? Please rank from most important to least important.

   Top Rank % / Average Rank

   43% / 2.4 That I get the information I was looking for (accuracy)
   28% / 2.5 Low cost / no cost to me
   23% / 2.6 The speed of response
   5% / 3.2 The amount of information I get back
   1% / 4.3 That I get the information digitally

8. How strongly do you feel the following public bodies should be legally required to notify you and/or the Office of the Information and Privacy Commissioner if your private information is breached?

   Agree (4,5) %

   82% The health sector (e.g., health authorities)
   78% The local government sector (e.g., cities and municipalities)
   75% Other public bodies (e.g., Crown corporations, professional associations, etc.)
   64% The education sector (e.g., K-12 school districts and postsecondary institutions)

9. For each of the scenarios below, which penalty seems most appropriate for the offense? (No penalty, Remedial action (education/awareness), Disciplinary action (suspension/termination), Fine less than $5,000, Fine between $5,001 and $50,000, Fine between $50,001 and $500,000, Charging of an offence including potential jail time)

   NET Discipline / Fine /Charge %

   94% Someone shares information they are not allowed to that benefits another person
   89% Someone collects client names through their work to benefit their side business
   79% Someone uses a government database to look up personal information about a celebrity, neighbour, or family member without a business reason to do so
   42% Someone shares information they are not allowed to because they didn't know it wasn't allowed.
   27% Someone accidentally sees the content of a personal file they shouldn't have

10. Do you have any other comments regarding B.C. Government Information Access and Privacy?

[Written responses not shown to protect the privacy of respondents.]

Appendix 3: Stakeholder consultation session details

Date	Method	Audience	Participating organizations
2021-05-28	ADM Roundtable	K-12 School Districts	Comox Valley School District Coquitlam School District Greater Victoria School District Maple Ridge - Pitt Meadows School District MyED BC Service Management Council Ministry of Education
2021-06-03	Minister Roundtable	Health Authorities and other representatives	Doctors of BC First Nations Health Fraser Health Island Health Northern Health Provincial Health Services Authority Vancouver Coastal Health Ministry of Health
2021-06-08	Minister Roundtable	BC Tech sector	Charitable Impact CoPilot AI Flawless Inbound Medimap Omnae Technologies Inc. Planetary Remote Sensing PressReader ReadyMode Riipen Networks Inc. SkyHive Sophos Streamline Athletes Ministry of Jobs, Economic Recovery and Innovation

2021-06-15	Stakeholder committee presentation	Ministry Privacy Officers	All government ministries
2021-06-15	Public survey on Information Access and Privacy	General public	Engagement occurred from June 15th to July 15th, 2021. 1786 responses were received.
2021-06-17	Stakeholder committee presentation	Information Security Advisory Council	All government ministries
2021-06-17	Stakeholder committee presentation	Ministry Chief Information Officers	All government ministries
2021-06-17	Minister Roundtable	Post-secondary Institutions	BC Institute of Technology College of New Caledonia Kwantlen Polytechnic University Research Universities' Council of BC University of British Columbia Thompson Rivers University University of Victoria Vancouver Community College Ministry of Advanced Education and Skills Training
2021-06-24	ADM Roundtable	Local governments	Capital Regional District City of Coquitlam City of Kamloops City of Langford City of Nanaimo City of New Westminster City of Surrey Cowichan Valley Regional District District of Fort St. James District of Highlands District of Sooke District of Tofino Local Government Management Association

			Regional District of Fraser-Fort George Regional District of Central Okanagan Regional District of East Kootenay Regional District of Kootenay Boundary Town of Qualicum Beach
2021-07-08	Stakeholder committee presentation	Broader Public Sector Chief Information Officers	Interior Health Authority BC Pension Corp Ministry of Health WorkSafeBC Ministry of Education BC Ferries ICBC Fraser Health VIHA CITZ OCIO Northern Health Authority BC Hydro TransLink BC Lottery Corporation PHSA FNHA
2021-07-21	Ipsos Omnibus survey on Information Access and Privacy	General public	Online survey of 800 adult (aged 18+) British Columbians fielded July 21 to 27, 2021.

PRIVACY SURVEY

Results Deck (DRAFT)

August 6, 2021

BRITISH COLUMBIA

Ipsos

Methodology

- Online survey of 800 adult (18+) British Columbians fielded July 21 to 27, 2021.
- Data has been weighted to reflect the British Columbia population age 18+ based on Census data for region, age, gender and education.
- The precision of Ipsos polls containing online data is measured using a credibility interval. In this case, the overall poll is accurate to within +/-4.0 percentage points, 19 times out of 20, had all British Columbia adults been polled.
  - The credibility interval will be wider among subsets of the population. All sample surveys and polls may be subject to other sources of error, including, but not limited to coverage error, and measurement error.
- Due to rounding:
  - Not all charts and tables in this report will add to exactly 100%.
  - Not all summary statistics will be exactly equal to the sum of their component parts.

DRAFT

SUMMARY OF RESULTS

DRAFT

Summary of Results

Services Accessed/Used in Past Year

The vast majority (91%) of British Columbians say they have accessed or used at least one provincial online service in the past year. The most used online services are booking a service appointment such as COVID or ICBC (63%), virtual doctor appointments (48%), lab test results (35%), paying government bills (35%) and applying for COVID benefits/supports (32%).

Ranking Importance in Accessing Government Services/Information

When thinking about accessing government services and information, British Columbians rank having government services available online as most important (33% rank #1). Next most important is up-to-date security protocols (25% rank #1), followed by Canadian data hosting/storage (17%) and quick delivery of services (16%).

Ranking Concern About Information Security Risks

By a wide margin, the top security concern of British Columbians is hackers stealing information or committing identity theft (62% rank #1). The top ranked secondary concerns include government using personal information in ways not consented to (15% rank #1) and organizations selling personal information (12%).

Ipsos
DRAFT

Summary of Results

Ranking Sensitivity of Information

Financial (49% rank #1) and health (28%) data/information stand out as the most sensitive types of personal information/data for British Columbians. Social services is a distant third (9% rank #1) for most sensitive type of personal information/data.

FOI Requests Made

Nearly two-in-ten (18%) British Columbians say have made a freedom of information (FOI) request for either their own information (14%) or for other government information (6%).

Ranking Importance When Seeking Government Info/Data

When seeking government information or data, British Columbians are most concerned with accuracy i.e., that they get the information they are looking for (42% rank #1). Other important attributes include getting information at low/no cost (28% rank #1) and the speed of response (23% rank #1).

DRAFT

Summary of Results

Agreement with Legal Requirement for Privacy Breach Notification

Most British Columbians support the idea that public bodies should be legally required to notify them and/or the Office of the Information and Privacy Commissioner if their private information is breached. Eight-in-ten say this legal requirement should be in place for the heath sector (82% agree) and the local government sector (78%). Slightly fewer agree this legal requirement is needed for the education sector (64% agree) or other public bodies (75%).

Appropriate Penalty by Scenario

A slight majority of British Columbians believe that the following privacy breaches should result in an offence charge or a monetary fine (as opposed to disciplinary action, remedial action or no penalty at all):

- Someone shares information they are not allowed to that benefits another person (56% say charge with offence or fine)
- Someone collects client names through their work to benefit their side business (56%).

Nearly half (47%) also believe an offence charge or fine is appropriate when someone uses a government database to look up personal information about a celebrity, neighbour, or family member without a business reason to do so.

Far fewer British Columbians think an offence charge or fine is appropriate when:

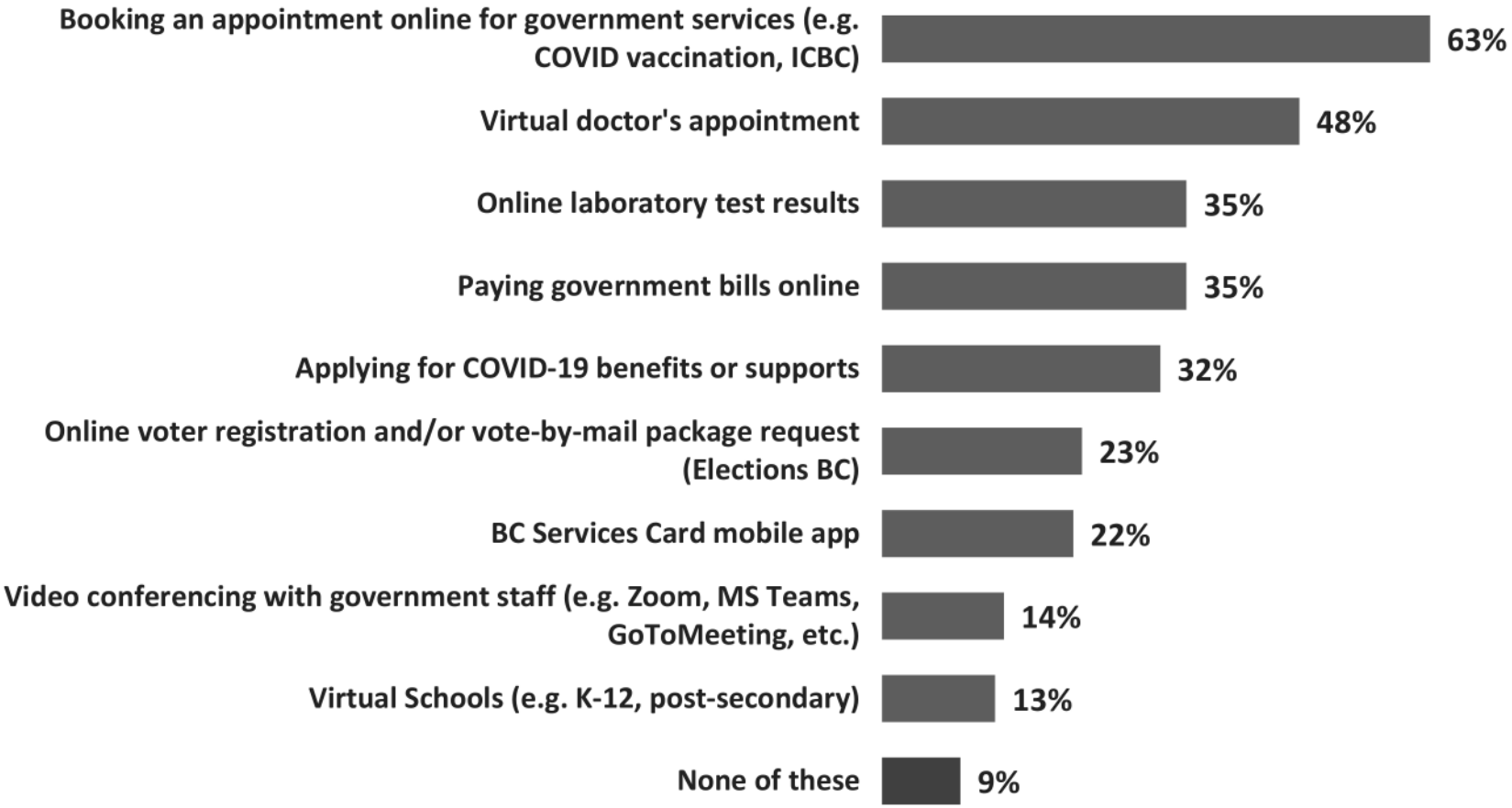
- Someone shares information they are not allowed to because they didn't know it (22% say charge with offence or fine)
- Someone accidentally sees the content of a personal file they shouldn't have (15%)

Ipsos
DRAFT

DETAILED RESULTS

DRAFT

Services Accessed/Used in Past Year



Q. *In the past year, which of the following have you accessed or used?*

Base: All respondents (n=800)

DRAFT

Services Accessed/Used in Past Year by Demos

	Total	Region			Age			Sex	
		Metro Vancouver	Vancouver Island	Interior/ North	18-34	35-54	55+	Male	Female
Sample Size	800	468	149	183	216	308	276	388	412
Booking an appointment online for government services (e.g. COVID vaccination, ICBC)	63%	67%	57%	58%	56%	65%	66%	60%	65%
Virtual doctor's appointment	48%	55%	45%	38%	45%	47%	51%	43%	53%
Online laboratory test results	35%	37%	33%	31%	26%	32%	45%	28%	41%
Paying government bills online	35%	39%	24%	32%	34%	39%	31%	38%	31%
Applying for COVID-19 benefits or supports	32%	32%	31%	31%	37%	34%	26%	31%	32%
Online voter registration and/or vote-by-mail package request (Elections BC)	23%	26%	20%	20%	19%	24%	26%	20%	26%
BC Services Card mobile app	22%	26%	16%	20%	30%	26%	13%	25%	20%
Video conferencing with government staff (e.g. Zoom, MS Teams, GoToMeeting, etc.)	14%	15%	13%	11%	17%	18%	6%	12%	15%
Virtual Schools (e.g. K-12, post-secondary)	13%	13%	15%	12%	24%	15%	2%	12%	14%
None of these	9%	6%	13%	12%	9%	8%	11%	9%	9%

Statistically higher **Statistically lower**

Q. *In the past year, which of the following have you accessed or used?*

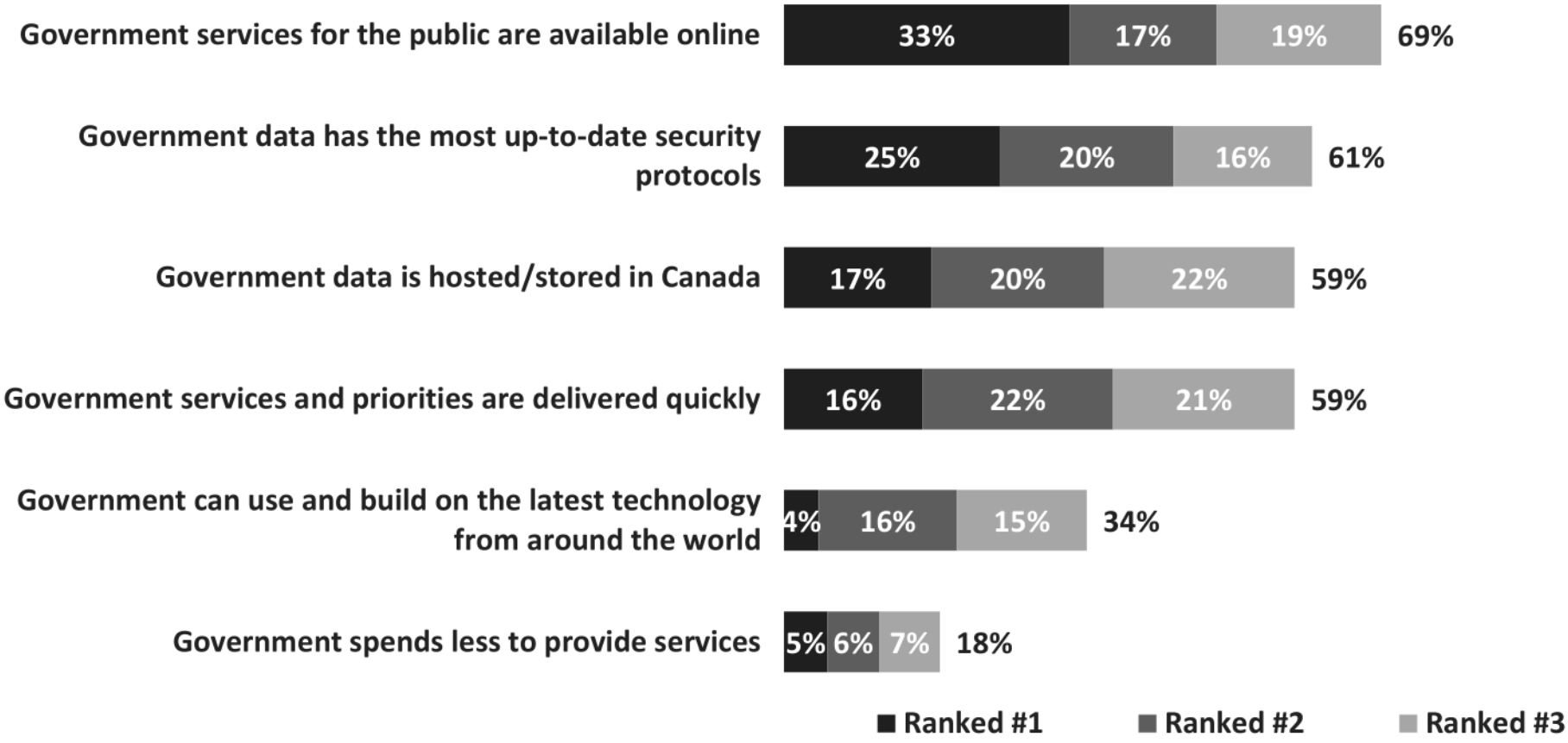
Base: All respondents (n=800)

Ipsos

DRAFT

Ranking Importance in Accessing Government Services/Information

(Top 3 Shown in Chart, But All Items Were Ranked)



Q. *When thinking about accessing government services and information, what is most important to you? Please rank the following elements from greatest to least importance.*

Base: All respondents (n=800)

Ipsos

DRAFT

Ranking Importance in Accessing Government Services/Information by Demos

Top 3 Ranking

	Total	Region			Age			Sex	
		Metro Vancouver	Vancouver Island	Interior/ North	18-34	35-54	55+	Male	Female
Sample Size	800	468	149	183	216	308	276	388	412
Government services for the public are available online	69%	70%	71%	66%	79%	67%	63%	69%	69%
Government data has the most up-to-date security protocols	61%	58%	62%	64%	49%	64%	68%	57%	65%
Government data is hosted/stored in Canada	59%	55%	59%	68%	51%	59%	67%	59%	60%
Government services and priorities are delivered quickly	59%	62%	52%	56%	51%	63%	60%	58%	59%
Government can use and build on the latest technology from around the world	34%	40%	29%	28%	50%	32%	24%	38%	31%
Government spends less to provide services	18%	14%	27%	18%	20%	16%	18%	19%	17%

Statistically higher **Statistically lower**

Q. *When thinking about accessing government services and information, what is most important to you? Please rank the following elements from greatest to least importance.*

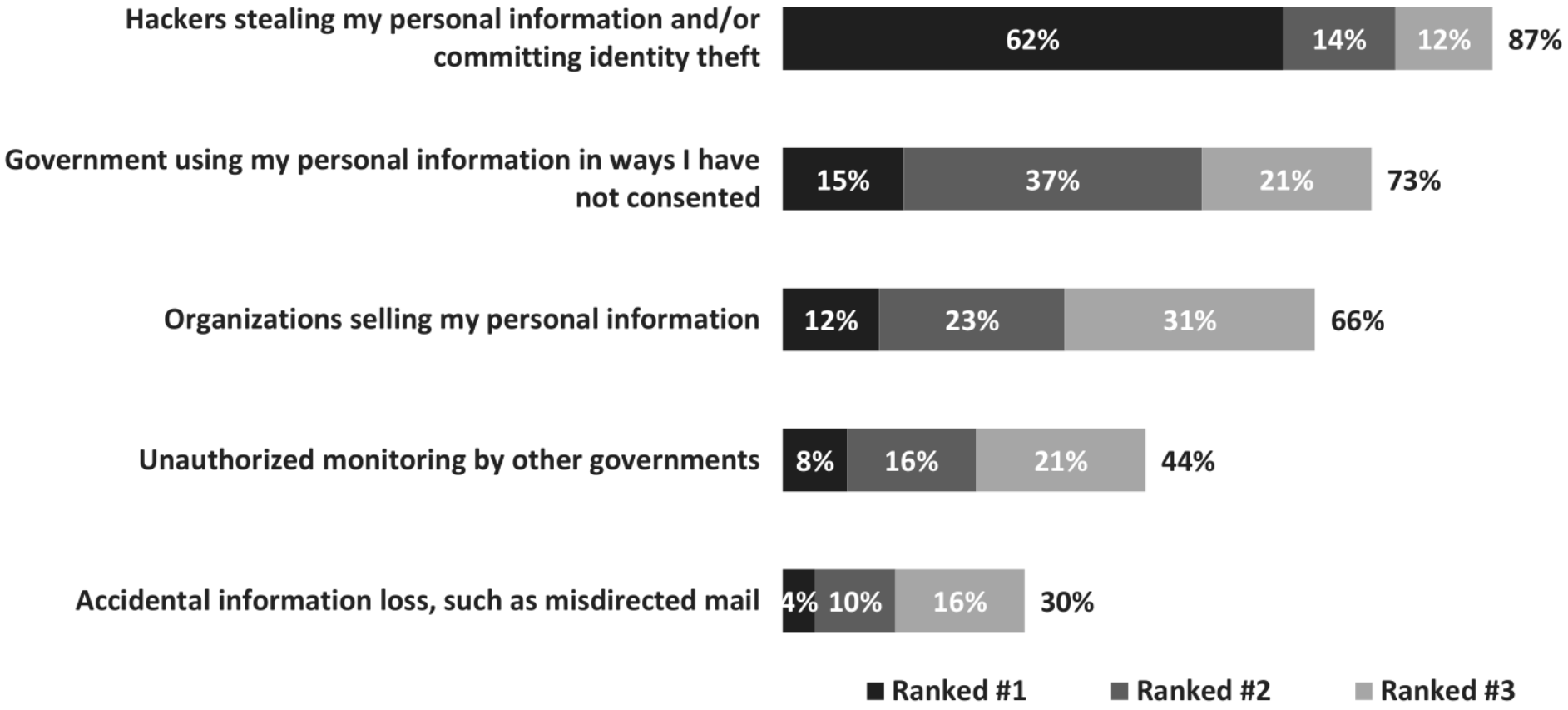
11 Base: All respondents (n=800)

Ipsos

DRAFT

Ranking Concern About Information Security Risks

(Top 3 Shown in Chart, But All Items Were Ranked)



Q. *How concerned are you about the following information security risks? Please rank the following elements from greatest concern to least concern.*

Base: All respondents (n=800)

DRAFT

Ranking Concern About Information Security Risks by Demos

Top 3 Ranking

	Total	Region			Age			Sex	
		Metro Vancouver	Vancouver Island	Interior/ North	18-34	35-54	55+	Male	Female
Sample Size	800	468	149	183	216	308	276	388	412
Hackers stealing my personal information and/or committing identity theft	87%	90%	88%	81%	88%	82%	91%	88%	86%
Government using my personal information in ways I have not consented	73%	71%	65%	81%	79%	73%	68%	71%	75%
Organizations selling my personal information	66%	66%	67%	66%	61%	67%	69%	66%	66%
Unauthorized monitoring by other governments	44%	42%	47%	45%	42%	46%	43%	44%	44%
Accidental information loss, such as misdirected mail	30%	31%	33%	27%	29%	32%	29%	31%	29%

Statistically higher **Statistically lower**

Q. *How concerned are you about the following information security risks? Please rank the following elements from greatest concern to least concern.*

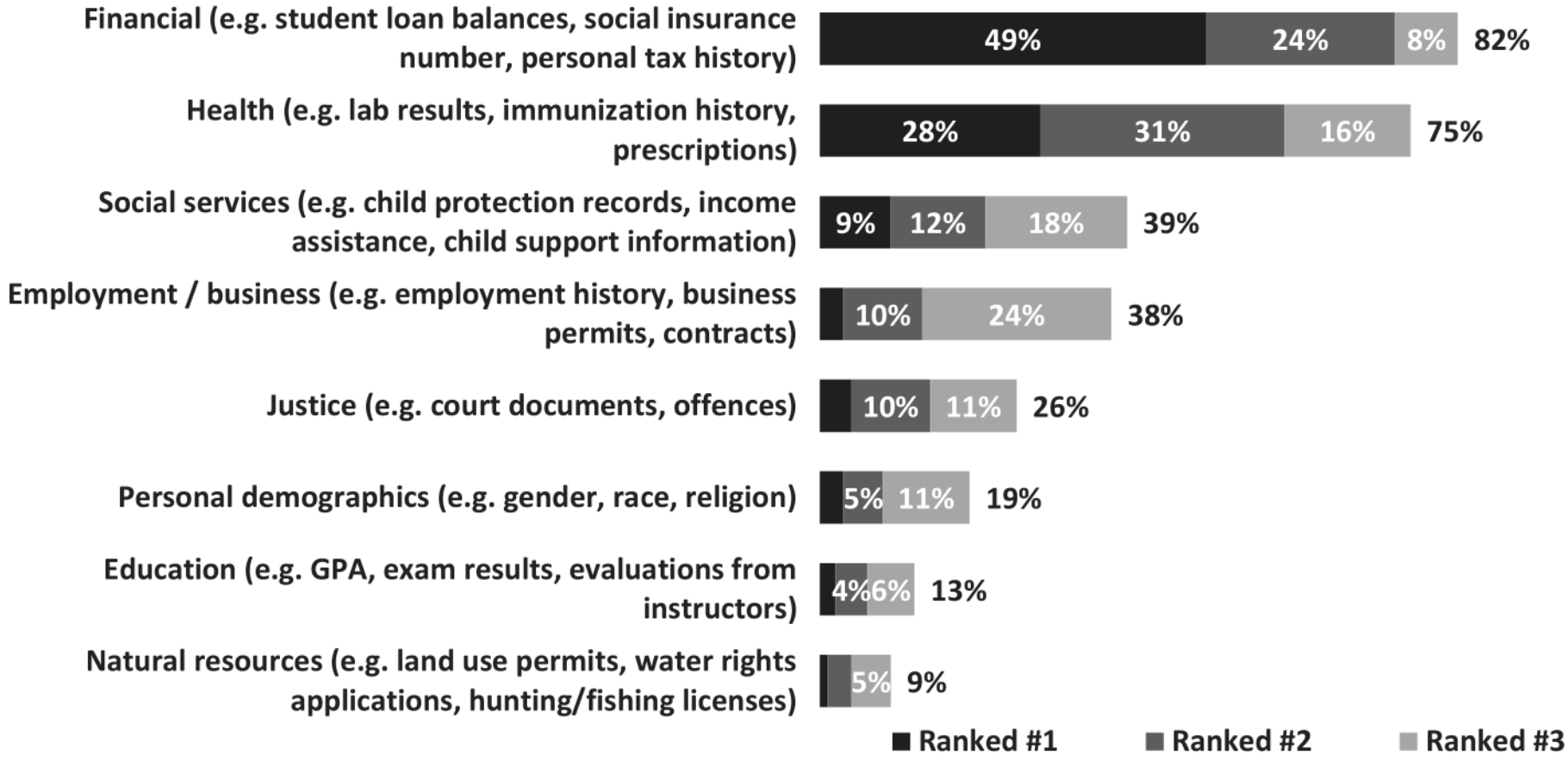
13 Base: All respondents (n=800)

Ipsos

DRAFT

Ranking Sensitivity of Information

(Top 3 Shown in Chart, But All Items Were Ranked)



Q. *When it comes to security, the more sensitive a piece of information or data is, the more strongly we should protect it. Reflecting on what is most important to you, how would you rank the sensitivity of the following personal information or data types? Please rank from most sensitive to least sensitive.*

Base: All respondents (n=800)

DRAFT

Ranking Sensitivity of Information by Demos

Top 3 Ranking

	Total	Region			Age			Sex	
		Metro Vancouver	Vancouver Island	Interior/ North	18-34	35-54	55+	Male	Female
Sample Size	800	468	149	183	216	308	276	388	412
Financial (e.g. student loan balances, social insurance number, personal tax history)	82%	80%	81%	86%	75%	83%	86%	83%	81%
Health (e.g. lab results, immunization history, prescriptions)	75%	76%	74%	73%	72%	72%	80%	76%	74%
Social services (e.g. child protection records, income assistance, child support information)	39%	35%	43%	44%	39%	39%	38%	33%	44%
Employment / business (e.g. employment history, business permits, contracts)	38%	40%	36%	34%	46%	41%	28%	43%	33%
Justice (e.g. court documents, offences)	26%	25%	30%	26%	25%	25%	28%	24%	28%
Personal demographics (e.g. gender, race, religion)	19%	19%	16%	19%	13%	18%	24%	17%	20%
Education (e.g. GPA, exam results, evaluations from instructors)	13%	16%	11%	8%	16%	13%	9%	12%	13%
Natural resources (e.g. land use permits, water rights applications, hunting/fishing licenses)	9%	9%	9%	11%	14%	9%	7%	12%	7%

Statistically higher **Statistically lower**

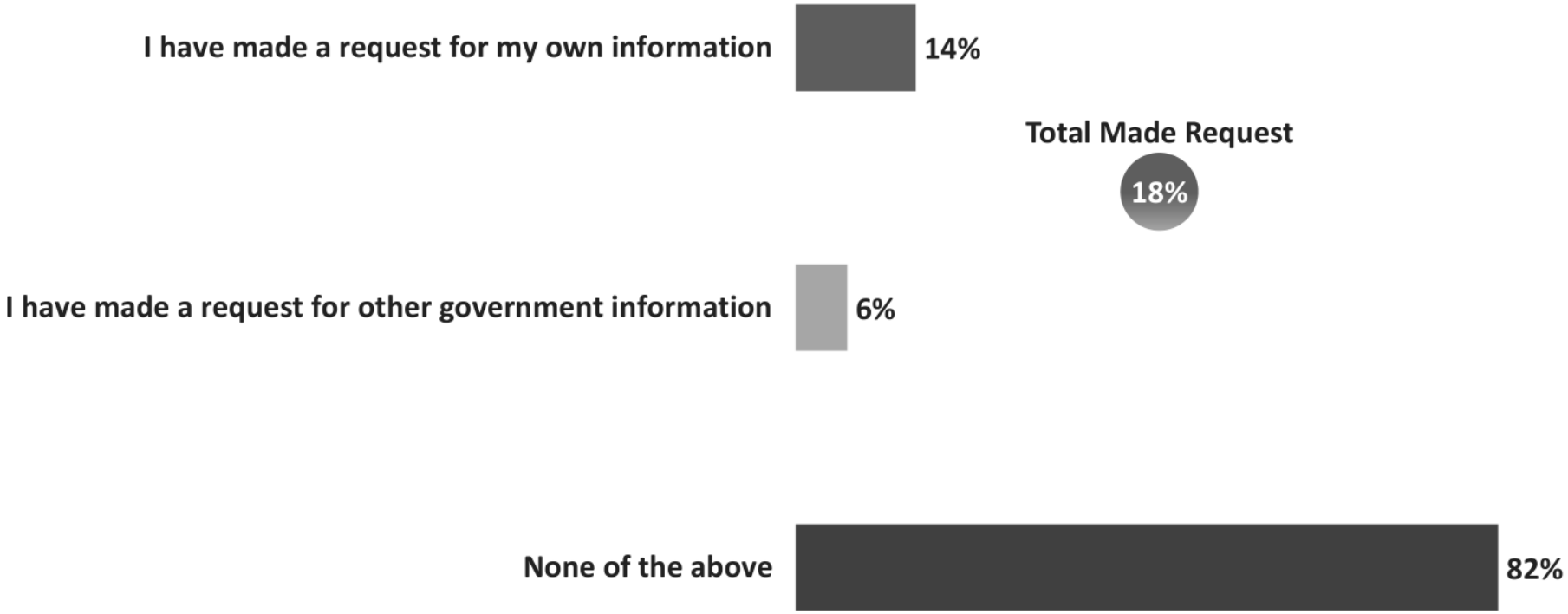
Q. *When it comes to security, the more sensitive a piece of information or data is, the more strongly we should protect it. Reflecting on what is most important to you, how would you rank the sensitivity of the following personal information or data types? Please rank from most sensitive to least sensitive.*

15 Base: All respondents (n=800)

Ipsos

DRAFT

FOI Requests Made



Q. *Which (if any) freedom of information (FOI) requests have you made?*

Base: All respondents (n=800)

DRAFT

FOI Requests Made by Demos

	Total	Region			Age			Sex	
		Metro Vancouver	Vancouver Island	Interior/ North	18-34	35-54	55+	Male	Female
Sample Size	800	468	149	183	216	308	276	388	412
I have made a request for my own information	14%	15%	14%	10%	18%	15%	8%	14%	13%
I have made a request for other government information	6%	6%	6%	6%	8%	6%	4%	7%	5%
None of the above	82%	81%	82%	84%	75%	80%	89%	81%	83%

Statistically higher **Statistically lower**

Q. *Which (if any) freedom of information (FOI) requests have you made?*

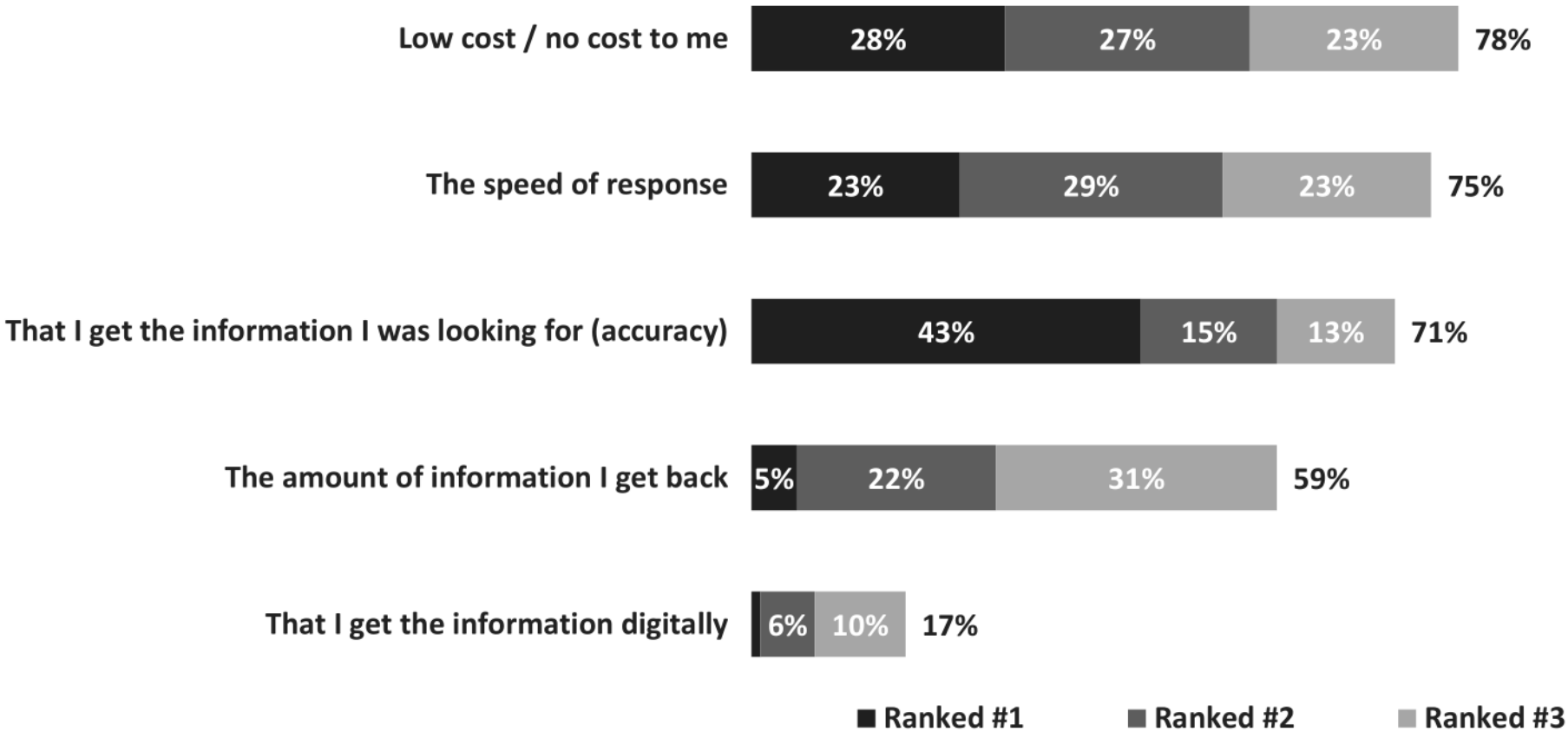
17 Base: All respondents (n=800)

Ipsos

DRAFT

Ranking Importance When Seeking Government Info/Data

(Top 3 Shown in Chart, But All Items Were Ranked)



Q. *How would you rank these in order of importance when seeking government information or data (i.e. not your own information)? Please rank from most important to least important.*

Base: All respondents (n=800)

DRAFT

Ranking Importance When Seeking Government Info/Data by Demos

Top 3 Ranking

	Total	Region			Age			Sex	
		Metro Vancouver	Vancouver Island	Interior/ North	18-34	35-54	55+	Male	Female
Sample Size	800	468	149	183	216	308	276	388	412
Low cost / no cost to me	78%	76%	77%	80%	79%	77%	78%	76%	80%
The speed of response	75%	79%	77%	68%	76%	74%	76%	75%	76%
That I get the information I was looking for (accuracy)	71%	67%	71%	77%	58%	72%	80%	67%	75%
The amount of information I get back	59%	56%	64%	61%	65%	60%	52%	63%	55%
That I get the information digitally	17%	22%	11%	13%	22%	17%	14%	20%	15%

Statistically higher **Statistically lower**

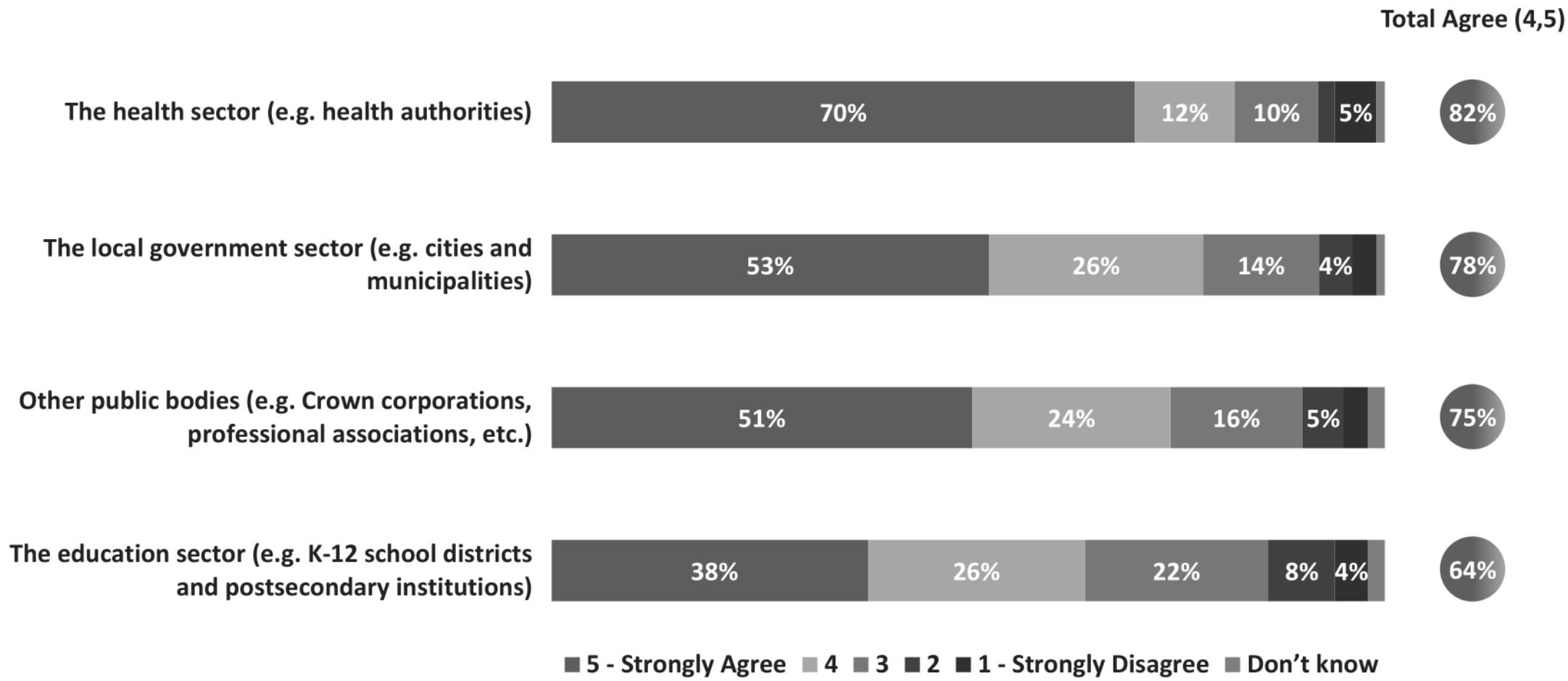
Q. *How would you rank these in order of importance when seeking government information or data (i.e. not your own information)? Please rank from most important to least important.*

19 Base: All respondents (n=800)

Ipsos

DRAFT

Agreement with Legal Requirement for Privacy Breach Notification



Q. *How strongly do you feel the following public bodies should be legally required to notify you and/or the Office of the Information and Privacy Commissioner if your private information is breached?*

20 Base: All respondents (n=800)

Ipsos

DRAFT

Agreement with Legal Requirement for Privacy Breach Notification by Demos

Total Agree (4,5)

	Total	Region			Age			Sex	
		Metro Vancouver	Vancouver Island	Interior/ North	18-34	35-54	55+	Male	Female
Sample Size	800	468	149	183	216	308	276	388	412
The health sector (e.g. health authorities)	82%	81%	80%	84%	68%	83%	92%	82%	82%
The local government sector (e.g. cities and municipalities)	78%	79%	78%	78%	74%	80%	80%	77%	79%
Other public bodies (e.g. Crown corporations, professional associations, etc.)	75%	75%	69%	77%	70%	76%	78%	74%	75%
The education sector (e.g. K-12 school districts and postsecondary institutions)	64%	64%	64%	63%	66%	69%	58%	64%	64%

Statistically higher **Statistically lower**

Q. *How strongly do you feel the following public bodies should be legally required to notify you and/or the Office of the Information and Privacy Commissioner if your private information is breached?*

21 Base: All respondents (n=800)

Ipsos

DRAFT

Appropriate Penalty by Scenario



Q. *For each of the scenarios below, which penalty seems most appropriate for the offence?*

22 Base: All respondents (n=800)

DRAFT

Appropriate Penalty by Scenario by Demos

Charge Offence / Fine (Total)

	Total	Region			Age			Sex	
		Metro Vancouver	Vancouver Island	Interior/ North	18-34	35-54	55+	Male	Female
Sample Size	800	468	149	183	216	308	276	388	412
Someone shares information they are not allowed to that benefits another person	56%	55%	57%	55%	61%	52%	55%	55%	55%
Someone collects client names through their work to benefit their side business	56%	59%	53%	53%	57%	53%	58%	57%	55%
Someone uses a government database to look up personal information about a celebrity, neighbour, or family member without a business reason to do so	47%	52%	40%	42%	49%	51%	40%	45%	48%
Someone shares information they are not allowed to because they didn't know it	22%	27%	18%	19%	29%	25%	16%	24%	22%
Someone accidentally sees the content of a personal file they shouldn't have	15%	18%	16%	9%	21%	17%	9%	18%	13%

Statistically higher **Statistically lower**

Q. *For each of the scenarios below, which penalty seems most appropriate for the offense?*

23 Base: All respondents (n=800)

Ipsos

DRAFT

Final Comments



Sampling of Comments

"For the most part, BC GIA does a whole range of services that I find useful."

"Government still hides data."

"I am tired of people getting away with this type of behaviour."

"I doubt that anything will work in favor of the public, only the government in regard to this."

"I have a huge lack of trust! "

"It seems to be quite confidential."

"It's a great service."

"It's a strong subject that our government must gather the best hackers in the world to prevent."

"Need to be much more transparent."

"Need to guard our data!!!"

"The government needs to do better in responding to FOI requests."

"The individual should be contacted if info pertaining them will be released to an organization other than gov."

"The sites often are not user friendly and difficult to contact assistance or to follow sometimes when they do reply."

Q. *Do you have any other comments regarding BC Government Information Access and Privacy?*

Base: All respondents (n=800)

Ipsos

DRAFT





DRAFT

BRITISH COLUMBIA | Ministry of Citizens' Services

Summary of discussion

FOIPPA Engagement - BC Technology Sector

June 8, 2021
11:00 am – 12:00pm

BC Government Attendees:
Lisa Beare, Minister of Citizens' Services
Brenda Bailey, Parliamentary Secretary for Technology and Innovation

Ministry of Citizens' Services
CJ Ritchie, Assoc. DM and GCIO
Kerry Pridmore, ADM, Corporate Information and Records Management
Matt Reed, ED, Strategic Policy & Legislation

Ministry of Jobs, Economic Recovery & Innovation
Maija Duffy, ED, Planning & Innovation

Tech Sector Attendees:
Jill Tipping, President and CEO, BC Tech Association
Alex Kroogman, CEO, PressReader
Amanda Mallow, Chief Human Resources Officer, Sophos
Blake Adam, CEO, Medimap
Brett Montrose, Founder & MD, Streamline Athletes
Caroline Dunn, CFO, SkyHive
Dan Lionello, Founder & CEO, Omnae Technologies Inc.
Dana Stephenson, CEO & Co Founder, Riipen Networks Inc.
James Zhan, Director of Product Management, CoPilot AI
John Bromley, Founder & CEO, Charitable Impact
Ramin Azar, CEO, Planetary Remote Sensing
Saher Ghattas, Founder, Flawless Inbound
Steve Chapman, Senior VP, Content Partnerships, PressReader
Sukh Basra, Founder, Readymode

Session purpose:

- Feedback on B.C.'s public sector privacy rules, specifically the current data residency requirements and opportunities for improvement.

Key themes:

- Access to cloud can improve service and increase small business competitiveness
    - Participants recognized the need to balance privacy for individuals with convenience and speed of response time for clients.
    - It was noted that the current data residency requirements limit access to faster, more powerful international cloud processing which would enable smaller companies and organizations to be more competitive.
- Focus on network security over location
    - There was general agreement that it is better to focus on protecting the network than focusing on where the network is located.
    - The EU General Data Protection Regulation (GDPR) is seen as the standard most companies are targeting which does allow for global, cloud-based systems.

  - Any changes B.C. contemplates will need to ensure it does not impact Canada's adequacy status / third country rating.
- Right security for the right information
  - A balanced, hybrid approach was supported by participants to ensure an appropriate level of security is applied to more or less private information.
  - This model would also support those companies who have developed niche businesses based on the current data residency requirements.

Information Access and Privacy 2021 Report Findings

Review period June 15th to July 15th 2021

Delivered by the Citizen Engagement Team
@govTogetherBC

Table of Contents

Introduction 3

Survey Responses and Demographic Data 3

Question: Currently, what is your primary source of information from government? 6

Question: Has your primary source of government information changed since the start of the pandemic (compared to before March 2020)? 8

Question: How has your primary source of government information changed since the start of the pandemic? 9

Question: In the past year, which of the following have you accessed or used? 11

Question: When thinking about accessing government services and information, what is the most important to you? 12

Question: Provide some detail on why the top-ranked option(s) you chose in the previous question are so important. 13

Question: How concerned are you about the following information security risks? 14

Question: When it comes to security, the more sensitive a piece of information or data is, the more strongly we should protect it. Reflecting on what is most important to you, how would you rank the sensitivity of the following personal information or data types? 15

Question: Which (if any) freedom of information (FOI) requests have you made? 16

Question: How would you rank these in order of importance when seeking government information or data (i.e., not your own information)? 17

Question: Provide some detail on why the top-ranked option(s) you chose in the previous question are so important. 18

Question: How strongly do you feel the following public bodies should be legally required to notify you and/or the Office of the Information and Privacy Commissioner if your private information is breached? 19

Question: For each of the scenarios below, which penalty seems most appropriate for the offense? 19

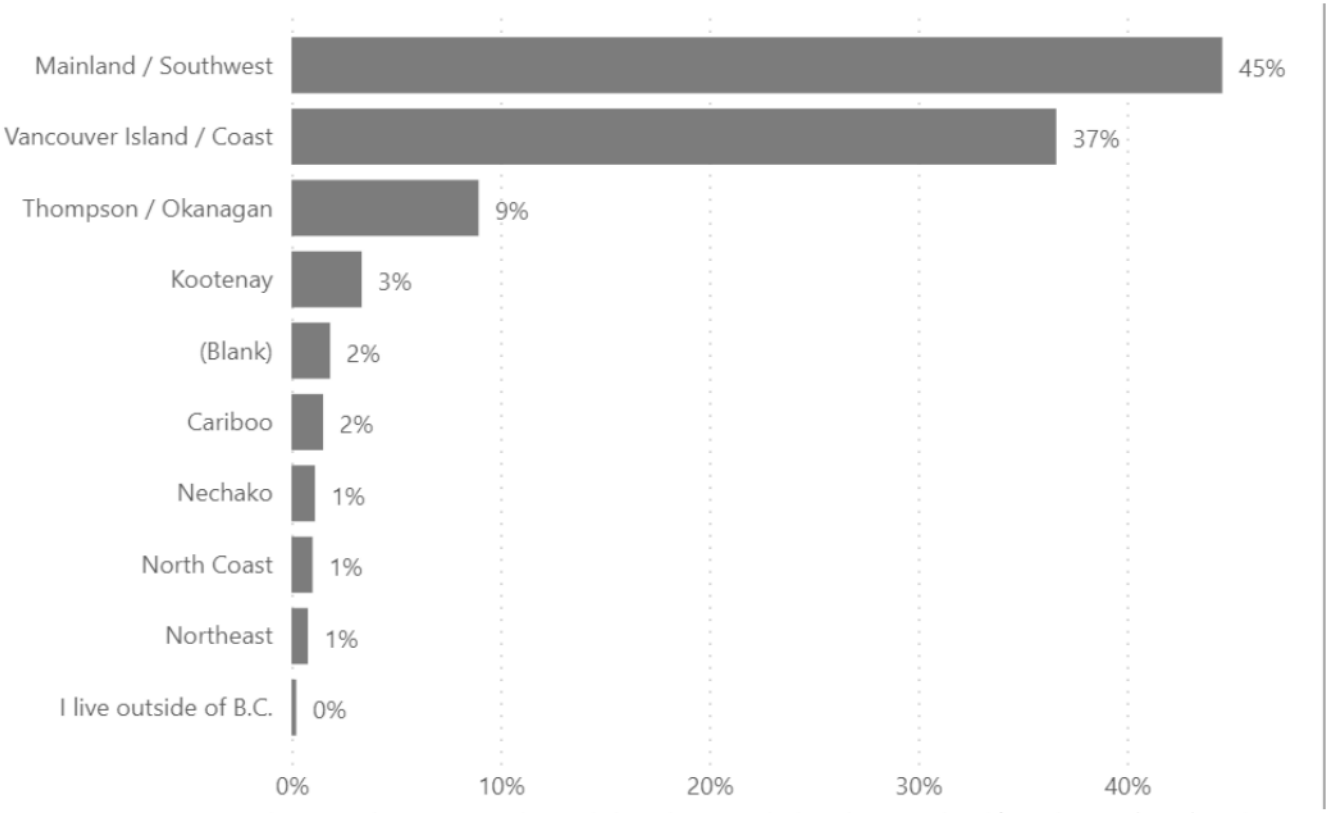
Question: If you have any further comments about access to government information and protection of privacy, please let us know. 21

Introduction

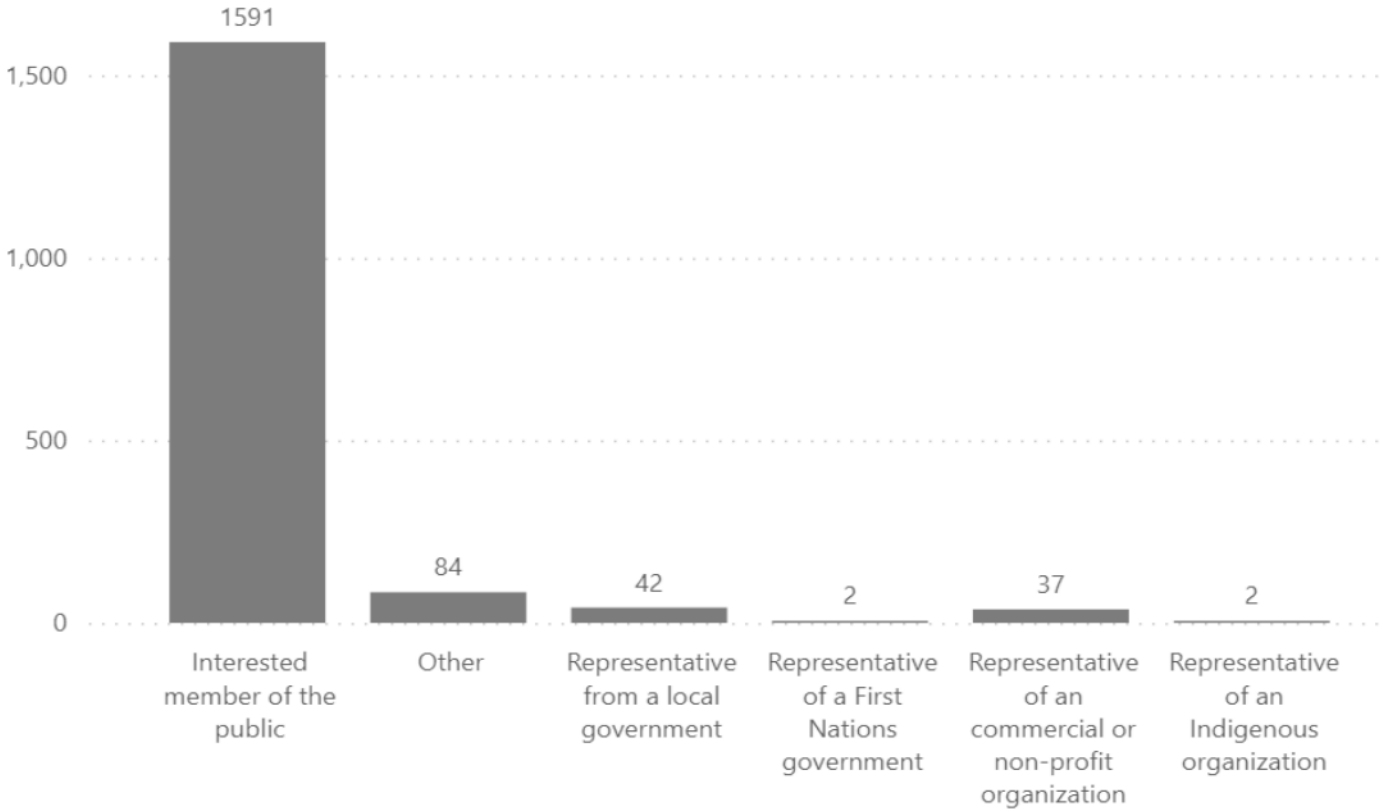
The following summary report is on the Information Access and Privacy 2021 engagement which occurred from June 15th to July 15th, 2021. The purpose of this engagement was to gather citizens' perspectives on how the COVID-19 pandemic has shifted how government does business and provides services to the general public. This report is based off raw survey data from 1786 responses provided by citizens. Each question included on the public survey will be represented within this report.

Survey Responses and Demographic Data

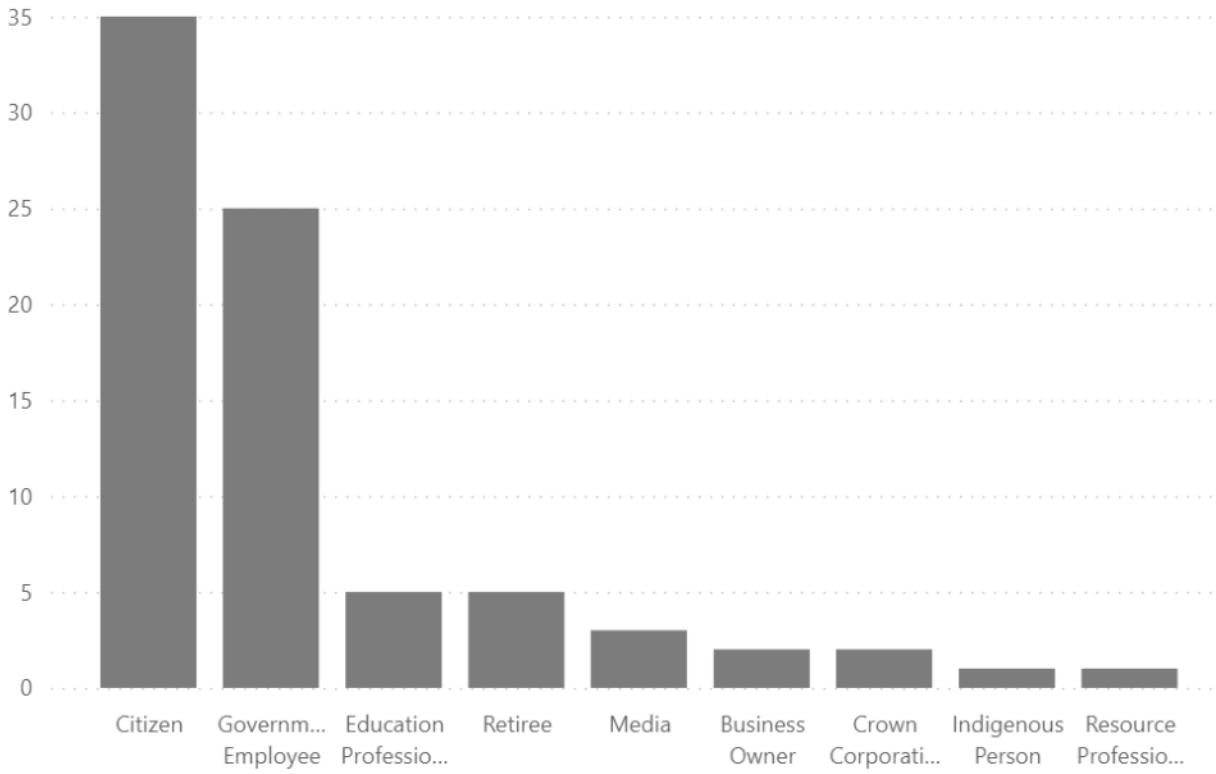
Full Responses	**1786**
Incomplete Responses	**667**
Total Responses	**2453**



Most respondents to the survey indicated that they resided in the Mainland/Southwest (45%) and Vancouver Island/Coast (37%) regions of British Columbia. Fewer respondents indicated that the resided in the Thompson/Okanagan (9%), Kootenay (3%), and Cariboo (2%) regions of British Columbia, with 1% of respondents indicated that they reside in the Nechako, North Coast, or Northeast regions of British Columbia. Less than 1% of respondents identified as residing outside of British Columbia with 2% of participants not responding to this question.



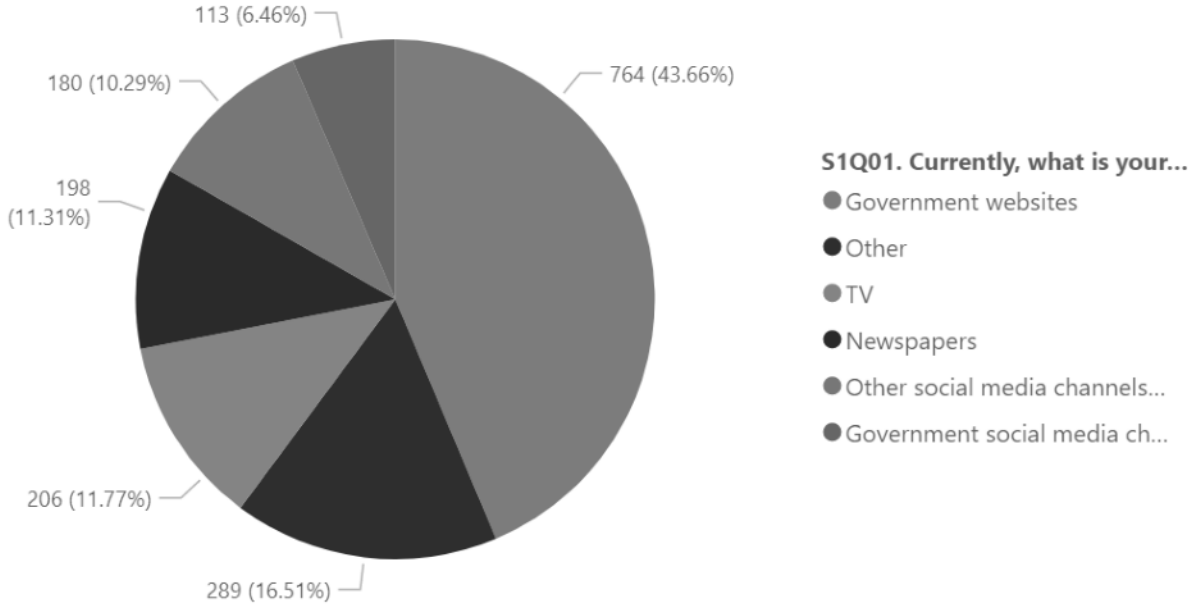
Almost all respondents to the survey identified as interested members of the public (1591). Further respondents identified as "other" (84), representatives from a local government (42), representatives of a commercial or non-profit organization (37), representative of a First Nations government (2), and representatives of an Indigenous organization (2).

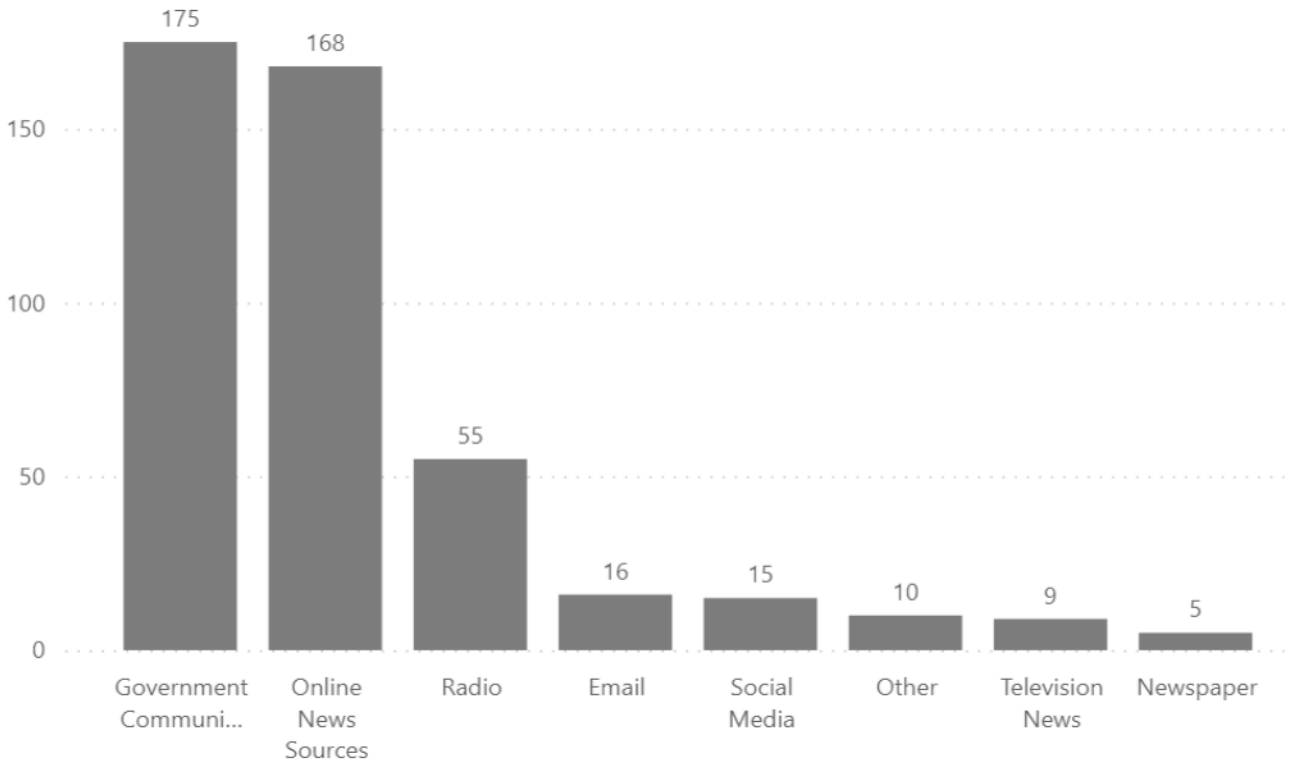


Respondents who selected “other” were categorized into the following groups: citizens (35), government employees (25), education professionals (5), retirees (5), media members (3), business owners (2), representatives of a crown corporation (2), an Indigenous person (1), and a resource professional (1)

Question: Currently, what is your primary source of information from government?

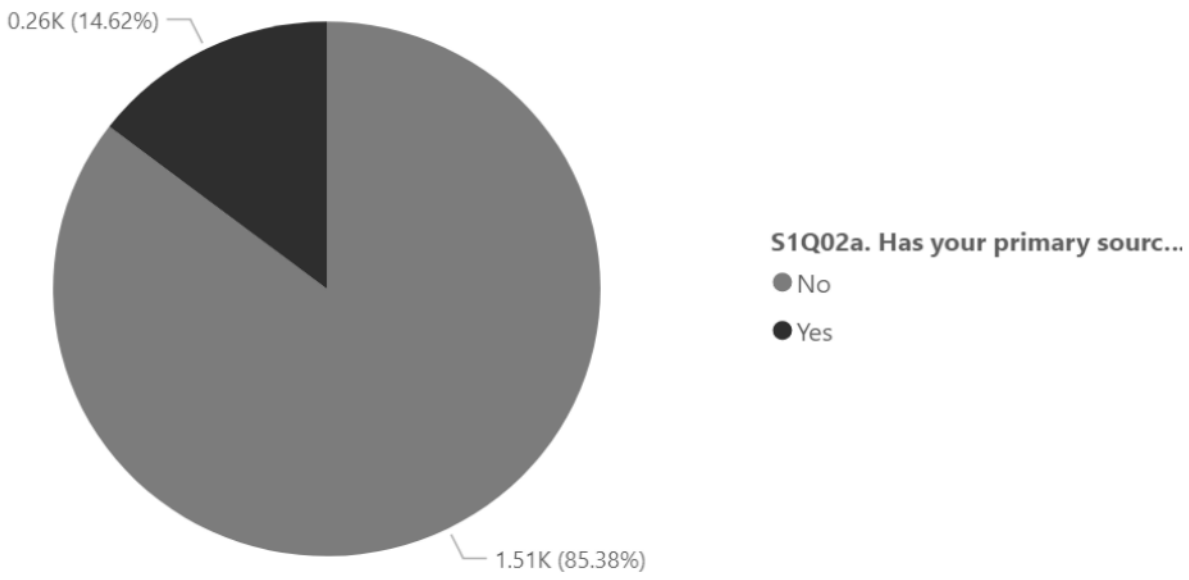
A significant percentage of respondents (43.66%) noted that government websites were their primary source of information from government. In comparison, 16.51% of participants responded that they used “other” sources to access government information, while fewer opted for TV (11.77%), newspapers (11.31%), other social media channels (10.29%), and government social media channels (6.46%).





Of the 278 participants who selected the "other" option for the previous question, the vast majority responded that government communications (175) and online news sources (168) were their primary sources of government information. Government communications included MLA reports and newsletters while online news sources included sites such as CBC and CTV.

Question: Has your primary source of government information changed since the start of the pandemic (compared to before March 2020)?

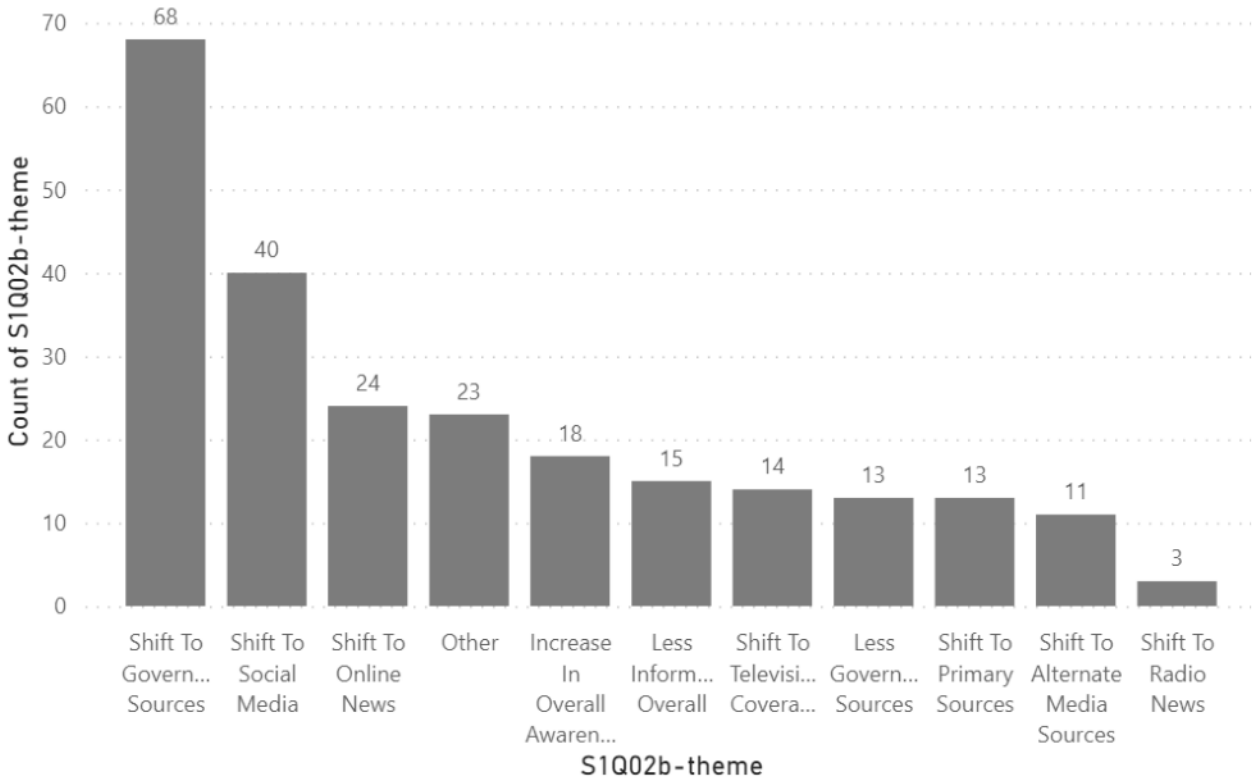


Most respondents (85.38%) indicated that their primary source of government information had not changed since March 2020. In contrast, a minority of respondents (14.62%) indicated that they had changed their primary source of government information since March 2020.

Question: How has your primary source of government information changed since the start of the pandemic?

The following word cloud shows the most common words identified in the responses to the question.





Across the responses to this question, several common themes emerged from the written comments. The top three themed responses were: *Shifts to Government Sources (68), Shifts to Social Media (40),* and *Shifts to Online News (24).*

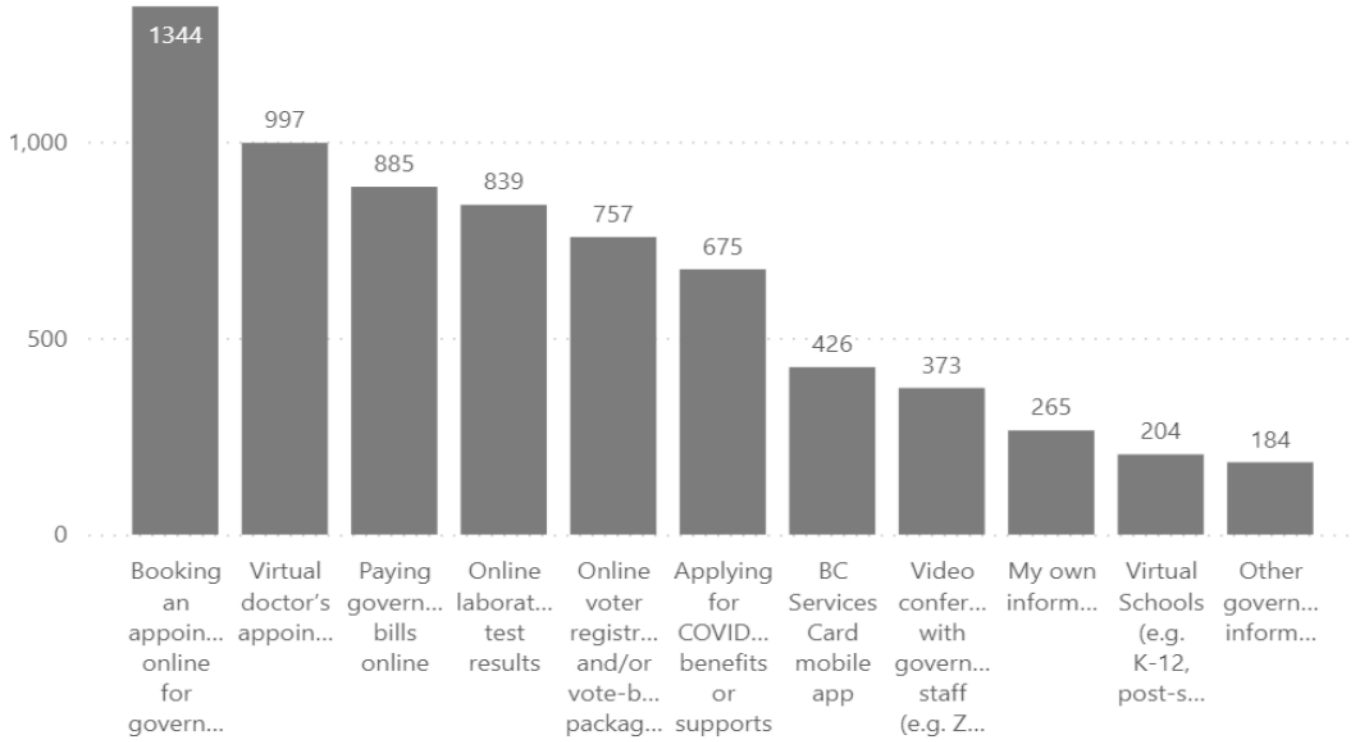
Within the *Shifts to Government sources* theme, respondents noted that they increasingly began to use government sources for information, mainly concerning the COVID-19 pandemic. Respondents mentioned that they had an increased interest in regular information updates from government, citing sources such as daily briefings from the Provincial Health Officer, BC Gov News, and the BC Centre for Disease Control.

For the *Shifts to Social Media* theme, participants expressed an increased usage in social media sites to receive information. Websites mentioned included Facebook, Twitter, Reddit, and YouTube, noting timely updates and accessibility as reasons for the shift.

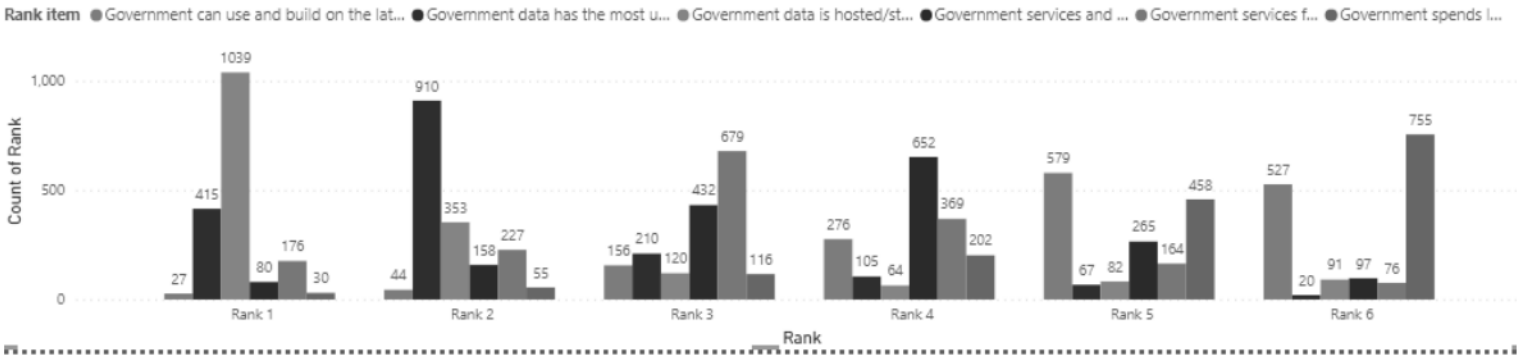
Finally, within the *Shifts to Online News* theme, respondents indicated that they now access much of their information via online news sites. Participants also noted that they had shifted away from analog forms of media including radio and television, instead opting for the convenience of online news.

Question: In the past year, which of the following have you accessed or used?

A significant number of respondents indicated that they had used services including booking an appointment online for government services, such as a COVID vaccination or ICBC (1344) or for a virtual doctor's appointment (997). Furthermore, many respondents used other services including paying government bills online (885), online laboratory results (839), and online voter registration and/or vote-by-mail page requests through Elections BC (675). Comparatively, fewer respondents noted that they had used the BC Services Card mobile app (426), video conferencing with government staff (373), their own information (265), virtual schools (204), and other government information (184).



Question: When thinking about accessing government services and information, what is the most important to you?



In responding to this question, participants overwhelmingly indicated that government data being stored or hosted in Canada was of greatest importance. This was represented as most participants ranked government data being hosted in Canada of first (1039) and second (910) most importance. Accordingly, few participants ranked hosting data in Canada as unimportant compared to other aspects of information access.

Moreover, participants felt that government data having the most up-to-date security protocols important, as respondents ranked this of first (415), second (910), and third (210) importance. As with government data being hosted in Canada, few participants indicated that security protocols were unimportant aspects. Furthermore, many participants indicated that online government sources for the public were somewhat important, as this was ranked of second (227), third (679), and fourth (369) most important.

Comparatively, many respondents indicated that government services and priorities being delivered quickly, and that government can use and build on the latest technology from around the world were of lesser importance. Timeliness of government sources was ranked of fourth (652) and fifth (265) most important, whereas government accessing the latest technology was of fifth (579) and sixth (527) most important.

Finally, participants largely felt that government spending less to provide services was of least importance. Many participants ranked government spending of fifth (458) and sixth (755) most important, with few participants ranking this of top importance.

Question: Provide some detail on why the top ranked option(s) you chose in the previous question are so important.

Several common themes emerged in participants' responses to this question. These themes were *security, digital, access, and time.*

The theme of *security* was defined as any feedback related to the protection and safety of data, including data residency.

"BC Government should have a data residency requirement. It is the most important way to ensure data is lawfully protected within Canada, more favourably within BC. This allows for protection and ease of access to request changes or removal of data. Public bodies should not be enabled to reduce responsibilities to protecting data by moving it offshore or reducing levels of service and access as a result."

"In order to keep my data secure, it is important to me that it remain in Canada. Laws around digital privacy and use of information differ between countries and I prefer transparent information about where my data is storied and how it is secured. Privacy and digital security are most important to me."

Within the theme of *Digital,* respondents expressed the importance of accessing information and services digitally, expressing that this would assist in the FOI process and should ultimately be a standard when making requests.

"In today's world, all government services ought to be available online/digitally. Any personal information or sensitive data associated with the online services or held by the government ought to have effective security protections in place."

Access related to free and easy access of personal information for individuals. Respondents' views included that information should not only be easy to access but should also be accurate and useful once received. Moreover, this related strongly to information redaction and perceived secrecy within the FOI process.

"Accessibility and ease of use will allow more people to access services. It's also important we keep our information safe."

Time related to the timeliness of the request and the ability to provide information quickly and easily when urgently required. This theme also related to the time process when making an FOI request.

"Technology is always changing; the focus should be on delivering the needed services in a timely and effective manner."

Question: How concerned are you about the following information security risks?

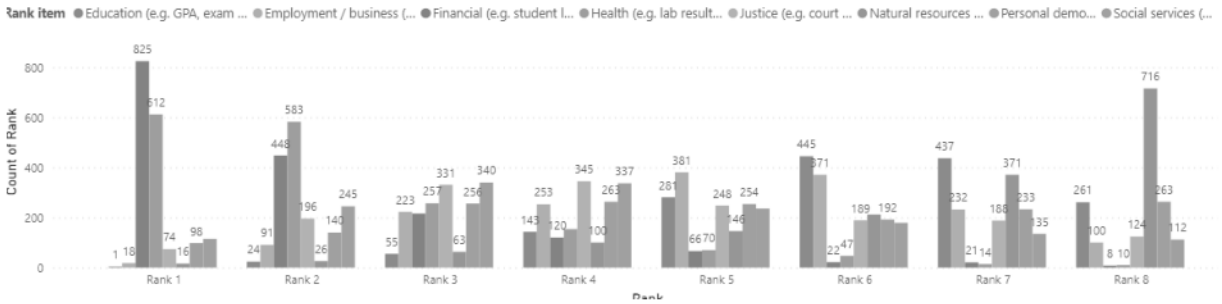


Participants responding to this question identified hackers stealing their personal information and/or committing identify theft (556), unauthorized monitoring by other governments (494) and government using their personal information in unconsented ways (488) and their primary concern around information security risks. This trend was further reflected as participants strongly ranked hacking and identity theft as their second (361) and third (342) concerns. Additionally, participants continued to rank unauthorized monitoring by other governments within their second (470) and third (380) concerns. As well, government use of personal information emerged strongly within the second (415) and third (356) rankings.

While organizations selling personal information was not largely ranked as a top concern (205), this risk was nevertheless prominent throughout later rankings. Participants ranked selling of personal information highly as a second (436) and third (502) concern. Although organizations selling personal information was not ranked as a top risk, participants still noted this as an area of concern.

In contrast, accidental information loss proved to be of least concern for participants. Accidental information loss was largely ranked as a fourth (378) and fifth (1031) concern by respondents. This was further reflected by the fact that a low number of participants ranked accidental information within their top three concerns.

Question: When it comes to security, the more sensitive a piece of information or data is, the more strongly we should protect it. Reflecting on what is most important to you, how would you rank the sensitivity of the following personal information or data types?



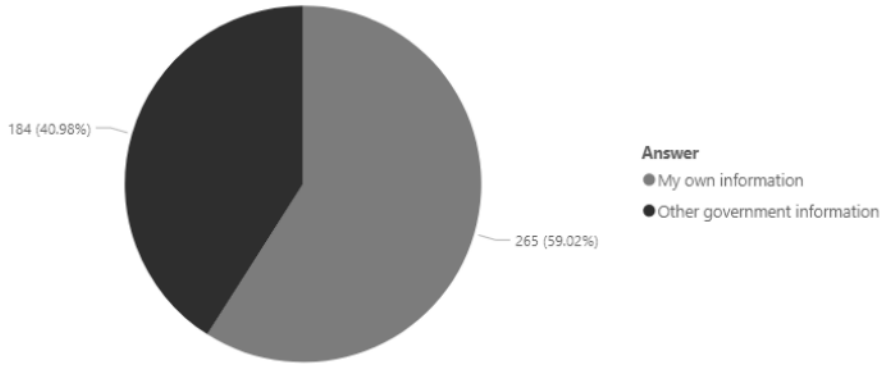
Participants responding to this question overwhelmingly viewed financial and health information as the most sensitive data types. Most respondents ranked financial data as either the most (825), or second most (448), sensitive data type. Health data was also viewed as very sensitive, with many respondents ranking health data as the most (612) or second most (448) sensitive data type. The sensitivity of financial and health data is further reflected by the fact that few participants ranked these as low-sensitivity data types.

Continuing, respondents tended to rank social services and justice data & information as medium-sensitivity data types. Participants ranked social services data as the third most (340) sensitive data type, with this trend continuing into the fourth (337), fifth (236), and sixth (179) rankings as well. Moreover, several respondents ranked social services as the most (115) and second-most (245) sensitive data type. Justice data followed a similar trend. Many respondents ranked justice data as the third most (331) sensitive data type, following into ranking justice data s the fourth (345), fifth (248), and sixth (189) most sensitive data type.

Personal demographics and employment data were also viewed by participants as medium-sensitivity data types. Participants ranked personal demographic information as the third most (256), fourth (263), fifth (254) and ,sixth-most (192) sensitive data type. Notably, several respondents ranked personal data as the seventh (233) and eighth-most (263) sensitive data type. Employment data was viewed through a similar lens, ranked as the third most (223), fourth (253), fifth (381), and sixth most (371) sensitive data type. However, unlike personal demographic data, fewer respondents ranked employment data as the seventh (232) or eighth most (100) sensitive data type.

By in large, participants largely viewed education and natural resource information as low-sensitivity data types. Respondents primarily ranked natural resource data as the eighth-most (716) sensitive data type, with education data largely ranked as the sixth (445), seventh (437), and eighth-most (261) sensitive as well.

Question: Which (if any) freedom of information (FOI) requests have you made?



The majority (59.02%) of participants responded that they requested their own information for freedom of information requests. In contrast, 40.98% of respondents answered that they were requesting other government information. These figures largely remained consistent for all respondents, to the survey. However, there was a shift in respondents who identified as representing a local government, with 55.56% of these respondents requesting other government information and 44.44% requesting their own information.

Question: How would you rank these in order of importance when seeking government information or data (i.e., not your own information)?

Rank item	Rank 1	Rank 2	Rank 3	Rank 4	Rank 5
The speed of response	170	478	554	352	164
The amount of information I get back	91	571	442	377	228
That I get the information I was looking for (accuracy)	1237	293	139	59	22
That I get the information digitally	49	141	208	392	881
Low cost / no cost to me	208	256	378	504	358

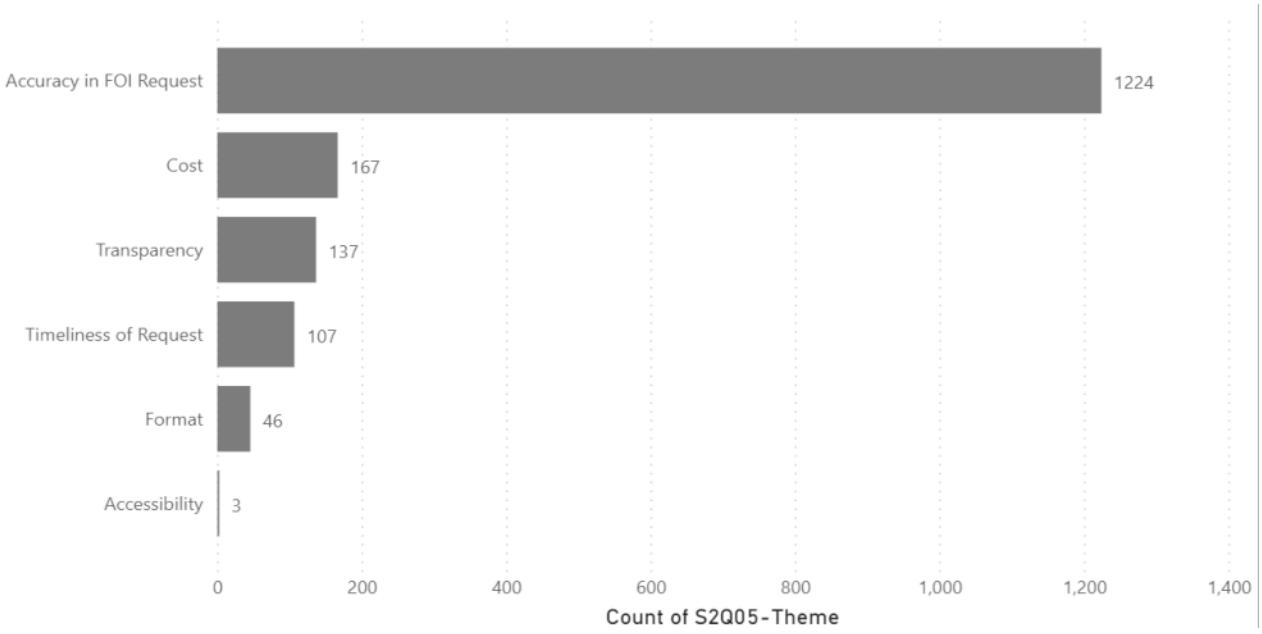
Participants strongly indicated that when seeking government information or data, accuracy of information was most important as many respondents ranked accuracy as the first most (1237) important aspect of seeking government data. In contrast, few respondents ranked accuracy as unimportant.

Moreover, participants felt that the amount of information received, and the speed of the response were important factors in seeking government information. Respondents ranked the amount of information as the second-most (571) and third-most (442) important aspect. In contrast to accuracy, there were significantly more respondents who viewed information received as less important, ranking this as the fourth-most (377) and fifth-most (228) important factors. A similar trend was seen in respondents who ranked the importance of the speed of the response. Respondents ranked speed as the second-most (478) and third-most (554) important aspect, but again many respondents viewed the speed of response as the fourth (352) or fifth (164) most important factor.

As with the amount of information and speed, participants ranked cost as a somewhat important factor. Respondents ranked cost as the second (256) and third (378) most important factor, however, many participants viewed cost as unimportant, emerging strongly as the fourth (504) and fifth (258) most important factor.

In contrast, participants largely viewed getting information in a digital format as unimportant when seeking government information. Respondents overwhelmingly ranked digital format as the fifth-most (881) important factor. Participants' views on the unimportance of digital format were further seen in the low number of respondents who ranked format within the top two ranks.

Question: Provide some detail on why the top ranked option(s) you chose in the previous question are so important.



Across the responses to this question, several common themes emerged from the written comments. The top three themed responses were: *Accuracy in FOI Request (1224), Cost (167),* and *Transparency (137).*

Responses tagged with the *Accuracy in FOI Request* theme were focused on ensuring that all FOI requests were accurate and fully met the needs requestor. Responses noted that accurately responding to an FOI request helps to build public trust, noting that transparency is reliant on accuracy itself.

"If I am seeking information, the most important thing is that the information is accurate. There's no point in low cost or speed if I cannot rely on that information."

"The goal of FOI is to ensure transparency and accountability for public bodies. Without accurate information, data is open for interpretation or require further FOI. Both of these add to additional financial costs for both the government and the requestor."

"*Without accuracy everything else is redundant."*

The theme of *Cost* covered responses that mentioned the current cost of making an FOI request in British Columbia. Responses ranged from noting that too high of a cost leads to inaccessibility for those

who may not be able to afford to make a request, while other responses noted that if the costs were reasonable, they would be willing to pay a fee for requests. Notably, many comments tagged with the theme of *Cost* also related to the previous theme of *Accuracy,* with respondents noting they would be willing to pay for FOI requests to ensure greater accuracy.

"Cost should not be a barrier to information access."

"I would rather the local government use the time needed to get me accurate results rather than rush the request and miss some records or provide them in such poor quality that they are useless. As long as the costs seem reasonable then there are no concerns."

"If I am requesting information, I would like to feel assured that the information I receive is complete and accurate. I would prefer it take longer to get a response and to pay for the time and energy and resources that civil servants used to obtain the information."

Within the theme of *Transparency*, responses largely expressed the idea that transparency should be the overall goal in the FOI process. Again, these comments related heavily to the themes of *Accuracy* and *Cost,* with responses noting that highly accurate and accessible information breeds transparency in government.

"Government transparency relies on the accuracy and completeness of information."

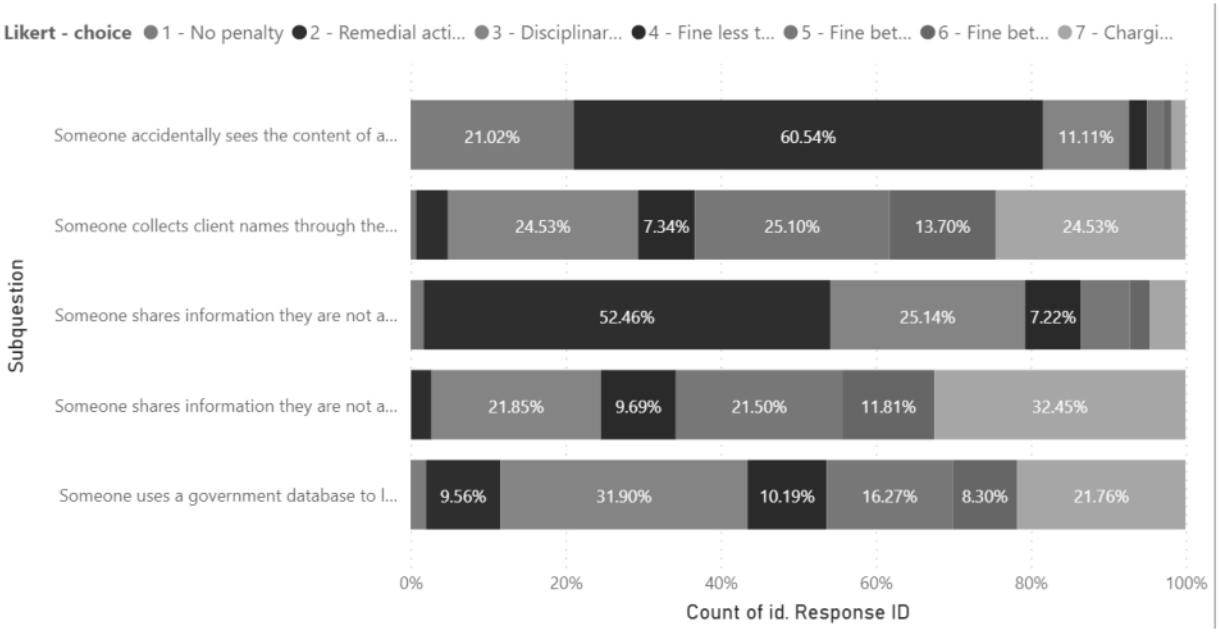
"Often with FOI, so much of the information is redacted that it has very little meaning when received by the person requesting the info. Governments need to be far more transparent and react more quickly for information that's requested. Government often use FOI requests as blatant opportunity to obfuscate, confuse, delay and deny citizens their rights under the Freedom of Information Act. Government should be held accountable by the courts for this lack of transparency."

"A well-informed public is of prime importance for democracies to function properly. Appropriate transparency is vital which means that there should not be over restriction of information based on possibility of embarrassing the government while maintaining privacy and security concerns where necessary."

Question: How strongly do you feel the following public bodies should be legally required to notify you and/or the Office of the Information and Privacy Commissioner if your private information is breached?

Participants heavily indicated that they would strongly agree that public bodies should notify a person or the OIPC if their private information was breached. This trend was consistent across all response options, with "strongly agree" emerging as the top answer for the local government sector (83.12%), the health sector (92.91%), the education sector (70.99%), and other public bodies (83.15%). Similarly, few respondents disagreed that public bodies should be legally required to notify a person about a privacy breach. These responses remained consistent across all groups of respondents (interested members of the public, local government representatives, etc.)

Question: For each of the scenarios below, which penalty seems most appropriate for the offense?



In responding to these options, participants largely felt that if someone used a government database to look up personal information without a business reason, disciplinary action (557) would be an appropriate penalty. Several participants also noted the charging an offence (380) would constitute as an appropriate response. The remaining respondents felt that fines between $5,001 and $50,000 (284), less than $5000 (178), or between $50,001 and $500,000 (145) or remedial action (167) would be appropriate, with few (35) respondents that no penalty would be appropriate.

Conversely, participants felt that if someone shared information that they were not allowed to which benefits another person that charging of an offense (566) would be an appropriate response.

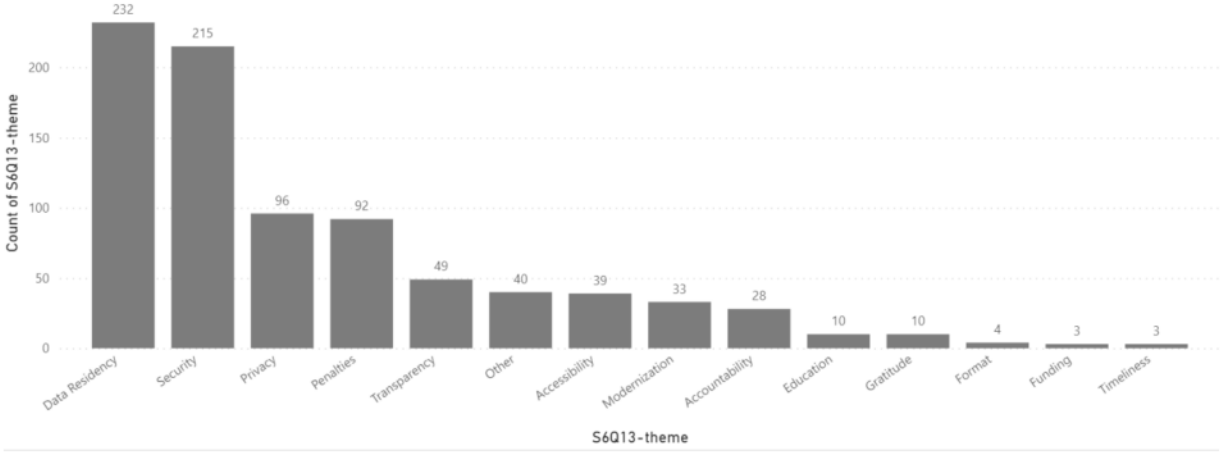
Respondents also noted that disciplinary action (381) would be an appropriate penalty. The remaining respondents agreed that a fine between $5,001 and $50,000 (375), between $50,001 and $500,000 (206), or less than $5,000 (381) would be an appropriate penalty. Few respondents believed that remedial action would be appropriate (45) with very few respondents (2) believing there should be no penalty for sharing information.

Moreover, participants strongly noted that if someone was to share information that they are not allowed to because they did not know it was not allowed, that remedial action (916) would be the best response. Many respondents also noted that disciplinary action (439) would be appropriate with other respondents agreeing that a fine less than $5000 (126), a fine between $5,001 and $50,000 (110, or charging of an offense (81) to be appropriate penalties. Few respondents felt that a fine between $50,001 and $500,000 (45) with fewer respondents feeling that no penalty (29) would be appropriate.

In contrast, participants largely felt that if someone collected client names through work to benefit their side business, that a fine between $5,001 and $50,000 (428), disciplinary action (428) or charging of an offense (428) to be appropriate actions. Other respondents noted that a fine between $50,001 and $500,000 (239) or a fine less than $5,000 (128) would be appropriate. Few respondents felt that remedial action (71) or no penalty at all (13) would constitute an appropriate response.

Finally, a vast majority of participants felt that if someone accidentally sees the contents of a personal file they should not have, that remedial action (1057) would be an appropriate penalty. Other respondents felt that no penalty (367) or disciplinary action (194) would be appropriate. Few respondents felt that a fine less than $5,000 (41), a fine between $5,001 and $50,000 (38), charging an offense (32), or a fine between $50,001 and $500,000 (17) to be appropriate responses.

Question: If you have any further comments about access to government information and protection of privacy, please let us know.



Across the responses to this question, several common themes emerged from the written comments. The top four themed responses were: *Data Residency (232), Security (215), Privacy (96), and Penalties (92).*

Within *Data Residency,* respondents' comments primarily stressed the importance of storing personal data in British Columbia and Canada. These respondents primarily identified as interested members of the public and largely called upon government to repeal the temporary suspension of the Data Residency Act as well as noting the strength of BC's privacy laws when compared to other jurisdictions. Moreover, respondents called for investment into BC's infrastructure to be able to support data residency and ensure that citizens' personal data can be stored in BC or Canada. The following sample comment echoes themes present in many participants' responses:

"The personal information of BC residents should not be allowed to leave Canada. This means that our sensitive data won't be subject to the intrusion of foreign governments, or handled in countries with weak privacy laws. It also means greater investment in Canada's information technology infrastructure. And all that means better privacy protections for all of us here in BC."

On the themes of *Security* and *Privacy,* respondents focused on ensuring that private data and information remains fully secure. Respondents noted that government should be protecting citizens' personal data with higher security levels compared to other organizations as well as holding government to higher standards concerning data protection. Additionally, respondents emphasized the consequences of personal data breaches and called for a strengthening of laws relating to privacy and security. Many responses also stressed the increasing significance of personal data as the world becomes more digital.

"Privacy is under attack in every form. Using commercial services and risk to privacy is a personal decision. But I consider Government held to a higher standard because some information must be kept by Government, and it has a duty to protect without consideration of profit."

"Privacy is fundamental to society, and more important now than ever given the emerging prevalence of surveillance capitalism and the digital nature of our lives. One of my top voting considerations is a party's stance on privacy, and I hope the BC government will continue to prioritize privacy over convenience."

Finally, for *Penalties* respondents noted the importance of clear guidelines and penalties around protection and misuse of personal data and information. Responses noted that government must do the utmost to ensure that personal data is not misused, stressing the value of personal information and data, calling for stricter penalties around privacy violations and ensuring actual enforcement. Suggested penalties ranged from an increase in monetary fines to actual jail time depending on the severity and context of the offense.

"Information has become a new commodity. Personal information is "personal", it should belong to the individual. Collecting information voluntarily is understandable, but selling it should be considered akin to violating intellectual property rights."

BRITISH COLUMBIA | Ministry of Citizens' Services

Summary of Discussion

FOIPPA Engagement - Health sector

June 2, 2021
4:00 – 5:00pm

BC Government Attendees:	*Ministry of Citizens' Services*	*Ministry of Health*
	Lisa Beare, Minister of Citizens' Services	Corrie Barclay, ADM, Health Sector IM/IT
	CJ Ritchie, Assoc. DM and GCIO	Paul Shrimpton, ED, Health IT Strategy and CIO
	Kerry Pridmore, ADM, Corporate Information and Records Management	Sukhy Sidhu, Senior Director, Privacy
	Matt Reed, ED, Strategic Policy & Legislation	Dr. Douglas Kingsford, Provincial Chief Medical Information Officer
Health Sector Attendees:	Stuart Bourhill, VP, Information Management, and Information Technology and CIO, First Nations Health	
	Dr. Shannon McDonald, A/Chief Medical Officer, First Nations Health	
	Jeff Hunter, CIO, Northern Health	
	Gregor McWalter, CIO, Fraser Health	
	Amyeen Hassanali, Fraser Health	
	Sandeep Mann, Fraser Health	
	Guy Weeks, Chief Technology Officer, Island Health	
	Dr. Mary-Lyn Fyfe, Chief Medical Information Officer, Island Health	
	Dr. Eric Grafstein, Chief Medical Information Officer, Vancouver Coastal Health	
	Ron Quirk, Vice Chair, Executive Vice President, Digital Information Services & Innovation, Provincial Health Services Authority and Vancouver Coastal Health	
	Dr. Alain Gagnon, Chief Medical Information Officer, Provincial Health Services Authority	
	Dawn Lake, Director, Digital Health Strategy, Doctors of BC	

Session purpose:

- Hear feedback on opportunities to improve B.C.'s public sector privacy rules with a focus on data residency, FOI, and privacy protection requirements.

Key themes:

- Data residency restrictions slowing health care reform and impacting ability to collaborate
  - COVID highlighted need to collaborate across jurisdictions – restrictions impact data flow
  - Addressing restrictions could improve access to human resources, address fiscal challenges and improve analytical resources
  - When working within current privacy requirements – often end up reducing functionality of a tool to a point where it doesn't meet the original needs
- Intersection between FOIPPA / PIPA s.12 and other acts
  - Need clarity on intersection between PIPA/FOIPPA s.12 – especially for FNHA and Doctors of BC
- Increasing FOI requests need to be addressed – taking time away from patients
  - Substantial increase during pandemic on all requests
  - Encourage review of fees – currently doesn't align with cost of processing a request

- Increasing access to patient information through portals could possibly reduce FOI requests but also potential for inadvertent misinterpretation of results. Will increase need for patient supports.
- Potential improvements could include broadening criteria to not respond to certain requests and reviewing/broadening criteria for 60-day extensions.

CITZ Media Request: FOIPPA - schedule 2

From:	Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Cc:	Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>, Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>, Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Sent:	October 19, 2021 4:06:11 PM PDT

For your approval

Reporter

Rob Shaw, Reporter
CHEK TV - Victoria
rshaw@cheknews.ca
250-893-0841

Deadline Tuesday, October 19, 2021 4:00 PM

Request

Have a Q about section 50 of the new Bill 22 on FOI.
It would appear to strike out "Office of the Premier and Executive Council Operations" from schedule 2 of the FOI act, which lists the public bodies that have to comply with FOI.
I briefly ran this by George in the PO and he said it's not what it appears, and there's a more technical explanation. Wondering if someone in the ministry could dig that up for me.
Trying to sort of boil it down to - does the change mean that if someone asked for records from a PO staffer or the premier in the future the PO would not have to respond?
But realize it first requires a more technical explanation of how it works now and the change, etc.

Recommendation

s.13

For MLB approval: CITZ Media Request: FOIPPA legislation - other jurisdictions

From: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Cc: Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Sent: October 19, 2021 5:53:29 PM PDT

Hi Kass, one last media request of the day for your review/MLB approval.
Program/HQ/Issues Management approved.

Reporter

Justin McElroy, Reporter
CBC - Victoria
justin.mcelroy@cbc.ca
250-384-2685 c: 604-346-6468

Deadline ASAP

Request

In light of Minister Beare frequently citing that similar jurisdictions to B.C. charge FOI fees between $5 and $50, reporter was wondering if the ministry could provide the specific list of jurisdictions that is being used as a reference point.

Recommendation: provide on background

B.C.'s fees are not yet set, but a modest fee is being recommended and will be determined through regulation soon.

Other jurisdictions:

- Alberta: $25 for first request - $50 per continuing request
- Saskatchewan: $20 per requests to local governments
- Ontario: $5 per request
- Nova Scotia: $5 per request
- Prince Edward Island: $5 per request
- Nunavut: $25 per request
- Canada: $5 per request.
- Manitoba, Quebec, New Brunswick, Newfoundland and Labrador, Yukon and Northwest Territories
  have no fees.

Re: FOR APPROVAL -- FW: CITZ Media Request: FOIPPA legislation - other jurisdictions

From: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX
Sent: October 19, 2021 6:03:52 PM PDT

Approved
Get Outlook for iOS
From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: Tuesday, October 19, 2021 6:00:03 PM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
Subject: FOR APPROVAL -- FW: CITZ Media Request: FOIPPA legislation - other jurisdictions
Media response below for your approval.
Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

Reporter
Justin McElroy, Reporter
CBC - Victoria
justin.mcelroy@cbc.ca
250-384-2685 c: 604-346-6468

Deadline ASAP

Request
In light of Minister Beare frequently citing that similar jurisdictions to B.C. charge FOI fees between $5 and $50, reporter was wondering if the ministry could provide the specific list of jurisdictions that is being used as a reference point.

Recommendation: provide on background

B.C.'s fees are not yet set, but a modest fee is being recommended and will be determined through regulation soon.

Other jurisdictions:

- Alberta: $25 for first request - $50 per continuing request
- Saskatchewan: $20 per requests to local governments
- Ontario: $5 per request
- Nova Scotia: $5 per request
- Prince Edward Island: $5 per request
- Nunavut: $25 per request
- Canada: $5 per request.
- Manitoba, Quebec, New Brunswick, Newfoundland and Labrador, Yukon and Northwest Territories
  have no fees.

Fwd: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

From:	Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Sent:	October 20, 2021 11:52:02 AM PDT
Attachments:	image007.jpg, image009.png, 2021-10-20 Letter to Minister Lisa Beare.pdf, image008.png

Get Outlook for iOS

From: Keira Morgan <KMorgan@oipc.bc.ca>
Sent: Wednesday, October 20, 2021 11:49 AM
To: 'Lisa.Beare@gov.bc.ca'
Cc: s.17 'Shauna.Brouwer@gov.bc.ca'; Kerry.Pridmore@gov.bc.ca
Subject: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

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

Good afternoon Minister Lisa Beare,
I write with respect to the above-referenced matter and on behalf of Commissioner Michael McEvoy. Attached please find a letter to you from the Commissioner dated October 20, 2021.
If you have any difficulty opening or viewing the attached PDF, please do not hesitate to contact me at your convenience.
Kind regards,

Keira Morgan
Executive Coordinator
She/Her/Hers
Phone: 250-387-0777
www.oipc.bc.ca

We acknowledge the homelands of the Indigenous Peoples of this place we now call British Columbia, and honour the many territorial keepers of the Lands on which we work.

This email and any attachments are only for the use of the intended recipient and must not be distributed, disclosed, used or copied by or to anyone else. If you receive this in error please contact the sender by return email and delete all copies of this email and any attachments.

Fwd: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

From:	Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX, Scott, Samantha CITZ:EX
Sent:	October 20, 2021 11:52:02 AM PDT
Attachments:	image008.png, image009.png, 2021-10-20 Letter to Minister Lisa Beare.pdf, image007.jpg

Get Outlook for iOS

From: Keira Morgan <KMorgan@oipc.bc.ca>
Sent: Wednesday, October 20, 2021 11:49 AM
To: 'Lisa.Beare@gov.bc.ca'
Cc: s.17 'Shauna.Brouwer@gov.bc.ca'; Kerry.Pridmore@gov.bc.ca
Subject: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

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

Good afternoon Minister Lisa Beare,
I write with respect to the above-referenced matter and on behalf of Commissioner Michael McEvoy. Attached please find a letter to you from the Commissioner dated October 20, 2021.
If you have any difficulty opening or viewing the attached PDF, please do not hesitate to contact me at your convenience.
Kind regards,

Keira Morgan
Executive Coordinator
She/Her/Hers
Phone: 250-387-0777
www.oipc.bc.ca

We acknowledge the homelands of the Indigenous Peoples of this place we now call British Columbia, and honour the many territorial keepers of the Lands on which we work.

This email and any attachments are only for the use of the intended recipient and must not be distributed, disclosed, used or copied by or to anyone else. If you receive this in error please contact the sender by return email and delete all copies of this email and any attachments.

FW: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

From:	Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>
To:	Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Cc:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent:	October 20, 2021 11:56:24 AM PDT
Attachments:	image007.jpg, image009.png, 2021-10-20 Letter to Minister Lisa Beare.pdf, image008.png

From: Keira Morgan <KMorgan@oipc.bc.ca>
Sent: October 20, 2021 11:49 AM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
Cc: s.17 Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Subject: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

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

Good afternoon Minister Lisa Beare,
I write with respect to the above-referenced matter and on behalf of Commissioner Michael McEvoy. Attached please find a letter to you from the Commissioner dated October 20, 2021.
If you have any difficulty opening or viewing the attached PDF, please do not hesitate to contact me at your convenience.
Kind regards,

Keira Morgan
Executive Coordinator
She/Her/Hers
Phone: 250-387-0777
www.oipc.bc.ca

We acknowledge the homelands of the Indigenous Peoples of this place we now call British Columbia, and honour the many territorial keepers of the Lands on which we work.

This email and any attachments are only for the use of the intended recipient and must not be distributed, disclosed, used or copied by or to anyone else. If you receive this in error please contact the sender by return email and delete all copies of this email and any attachments.

FW: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

From:	Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
To:	Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>, Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Sent:	October 20, 2021 11:58:14 AM PDT
Attachments:	image007.jpg, image009.png, 2021-10-20 Letter to Minister Lisa Beare.pdf, image008.png

FYI

From: Keira Morgan <KMorgan@oipc.bc.ca>
Sent: October 20, 2021 11:49 AM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>
Cc: s.17 Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Subject: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

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

Good afternoon Minister Lisa Beare,
I write with respect to the above-referenced matter and on behalf of Commissioner Michael McEvoy. Attached please find a letter to you from the Commissioner dated October 20, 2021.
If you have any difficulty opening or viewing the attached PDF, please do not hesitate to contact me at your convenience.
Kind regards,

Keira Morgan
Executive Coordinator
She/Her/Hers
Phone: 250-387-0777
www.oipc.bc.ca

We acknowledge the homelands of the Indigenous Peoples of this place we now call British Columbia, and honour the many territorial keepers of the Lands on which we work.
This email and any attachments are only for the use of the intended recipient and must not be distributed, disclosed, used or copied by or to anyone else. If you receive this in error please contact the sender by return email and delete all copies of this email and any attachments.

Re: FYI: OIPC BC: Letter to Minister Beare re: Bill 22: Freedom of Information and Protection of Privacy Act amendments

From:	Olson, Michael GCPE:EX <Michael.Olson@gov.bc.ca>
To:	Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Cc:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>, Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>, Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>, Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>, Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>, Williams, Susan GCPE:EX <Susan.Williams@gov.bc.ca>
Sent:	October 20, 2021 12:33:48 PM PDT

s.13

– – – – –

Michael Olson
Issues Manager
(250) 893-2046

On Oct 20, 2021, at 12:14 PM, Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca> wrote:

s.13

From: Rob Shaw <rshaw@cheknews.ca>
Sent: October 20, 2021 12:12 PM
To: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Subject: Fwd: OIPC BC: Letter to Minister Beare re: Bill 22: Freedom of Information and Protection of Privacy Act amendments

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

Hey there,
Hoping the minister can respond to this today. 7 pages of detailed concerns about the bill. Does gov intend to pause this legislation in response, or amend it, or proceed, etc?
Thanks,
Rob

---------- Forwarded message ---------
From: **Michelle Mitchell** <MMitchell@oipc.bc.ca>
Date: Wed, Oct 20, 2021 at 11:51 AM
Subject: OIPC BC: Letter to Minister Beare re: Bill 22: Freedom of Information and Protection of Privacy Act amendments
To: Michelle Mitchell <MMitchell@oipc.bc.ca>

Please find below a letter from Commissioner McEvoy to Minister Beare, published on our website today:

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.[1] 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, 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,

ORIGINAL SIGNED BY

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

---

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

FOI - CTZ-2021-13473 (due Oct 25)

From: McEwen, Shaylene CITZ:EX <Shaylene.McEwen@gov.bc.ca>
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 20, 2021 2:27:59 PM PDT

Hi Kass,

FOI: CTZ-2021-13473 has been returned from the IAO for review/approval prior to DM's final sign off. (Apologies received on the short turnaround)

Z:\5. SMA - FINAL SIGN-OFFs\CTZ-2021-13473 (IAO Redlined – Final Review and sign off)
Redline CTZ-2021-13473 (IAO Redline)

Thank you,
Shay

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

From:	Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
To:	Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent:	October 20, 2021 6:29:15 PM PDT
Attachments:	image002.png, image003.png, image001.jpg

Really appreciate that – thank you.

From: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Sent: October 20, 2021 6:28 PM
To: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Subject: RE: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

MLB just came in and asked that I send along her appreciation, as well. She thought the bullets were great!

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Lawal, Kassandra CITZ:EX
Sent: October 20, 2021 6:18 PM
To: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Cc: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>; Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Subject: RE: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

These are really excellent bullets, Kerry. Many thanks for putting them together so quickly and running through short answers for MLB this afternoon.

Much appreciated!

Kass

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Sent: October 20, 2021 5:42 PM
To: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Cc: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Ritchie, CJ CITZ:EX <CJ.Ritchie@gov.bc.ca>; Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>; Scott, Samantha CITZ:EX <Samantha.Scott@gov.bc.ca>
Subject: RE: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

Apologies, we thought this came over earlier. Specific bullets to the items raised in the letter.

Kerry Pridmore | Assistant Deputy Minister |
Corporate Information and Records Management Office |
Ministry of Citizen Services |
Cell: 250-507-1485 |

From: Lawal, Kassandra CITZ:EX Kassandra.Lawal@gov.bc.ca
Sent: October 20, 2021 12:01 PM
To: Pridmore, Kerry CITZ:EX Kerry.Pridmore@gov.bc.ca
Cc: Brouwer, Shauna CITZ:EX Shauna.Brouwer@gov.bc.ca
Subject: RE: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

We're on it. Asked Kirsten to work with you re bullets responding to all the items he has laid out in the letter.

Kassandra Lawal
Office 778-974-6009 | Cell 778-678-3776
kassandra.lawal@gov.bc.ca

From: Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>
Sent: October 20, 2021 11:56 AM
To: Youngs, Kirsten R GCPE:EX <Kirsten.Youngs@gov.bc.ca>
Cc: Lawal, Kassandra CITZ:EX <Kassandra.Lawal@gov.bc.ca>
Subject: FW: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments
From: Keira Morgan <KMorgan@oipc.bc.ca>
Sent: October 20, 2021 11:49 AM
To: Beare, Lisa CITZ:EX <Lisa.Beare@gov.bc.ca>

Cc: s.17 Brouwer, Shauna CITZ:EX <Shauna.Brouwer@gov.bc.ca>; Pridmore, Kerry CITZ:EX <Kerry.Pridmore@gov.bc.ca>
Subject: Bill 22 - Freedom of Information and Protection of Privacy Act Amendments

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

Good afternoon Minister Lisa Beare,

I write with respect to the above-referenced matter and on behalf of Commissioner Michael McEvoy. Attached please find a letter to you from the Commissioner dated October 20, 2021.

If you have any difficulty opening or viewing the attached PDF, please do not hesitate to contact me at your convenience.

Kind regards,

Keira Morgan
Executive Coordinator
She/Her/Hers
Phone: 250-387-0777
www.oipc.bc.ca

We acknowledge the homelands of the Indigenous Peoples of this place we now call British Columbia, and honour the many territorial keepers of the Lands on which we work.

This email and any attachments are only for the use of the intended recipient and must not be distributed, disclosed, used or copied by or to anyone else. If you receive this in error please contact the sender by return email and delete all copies of this email and any attachments.

Corporate Statistics

Fiscal Year	Requests Received	Requests Closed	On-Time Compliance
2015/16	9,261	8,805	74%
2016/17	9,296	9,856	80%
2017/18	10,471	9,362	90%
2018/19	12,245	11,787	89%
2019/20	13,054	12,907	83%
2020/21	10,268	10,840	85%
2021/22 YTD	4,806	4,742	81%

Ministry Statistics (bundled FY2017/18 to present)

Ministry	Requests Received	Requests Closed	On-Time Compliance
Advanced Education and Skills Training	794	793	88%
Agriculture, Food and Fisheries	1,000	978	87%
Attorney General	2,070	2,040	81%
Children and Family Development	10,419	9,714	79%
Citizens' Services	1,390	1,366	92%
Education	914	901	87%
Energy, Mines and Low Carbon Innovation	1,080	1,055	84%
Environment and Climate Change Strategy	1,814	1,807	86%
Finance	5,899	5,969	89%
Forests, Lands, Natural Resource Operations and Rural Development	2,454	2,354	81%
Health	2,226	1,938	78%
Indigenous Relations and Reconciliation	751	748	84%
Jobs, Economic Recovery and Innovation	1,029	1,034	74%
Labour	699	679	82%
Mental Health and Addictions	621	593	73%
Municipal Affairs	973	962	81%
Office of the Premier	3,224	3,195	93%
Public Safety and Solicitor General	6,367	6,402	93%
Social Development and Poverty Reduction	4,604	4,611	91%
Tourism, Arts, Culture and Sport	768	748	78%
Transportation and Infrastructure	1,748	1,735	92%

Corporate Statistics

Fiscal Year	Requests Received	Requests Closed	On-Time Compliance
2015/16	9,261	8,805	74%
2016/17	9,296	9,856	80%
2017/18	10,471	9,362	90%
2018/19	12,245	11,787	89%
2019/20	13,054	12,907	83%
2020/21	10,268	10,840	85%
2021/22 YTD	4,806	4,742	81%

Ministry Statistics (bundled FY2017/18 to present)

Ministry	Requests Received	Requests Closed	On-Time Compliance
Advanced Education and Skills Training	794	793	88%
Agriculture, Food and Fisheries	1,000	978	87%
Attorney General	2,070	2,040	81%
Children and Family Development	10,419	9,714	79%
Citizens' Services	1,390	1,366	92%
Education	914	901	87%
Energy, Mines and Low Carbon Innovation	1,080	1,055	84%
Environment and Climate Change Strategy	1,814	1,807	86%
Finance	5,899	5,969	89%
Forests, Lands, Natural Resource Operations and Rural Development	2,454	2,354	81%
Health	2,226	1,938	78%
Indigenous Relations and Reconciliation	751	748	84%
Jobs, Economic Recovery and Innovation	1,029	1,034	74%
Labour	699	679	82%
Mental Health and Addictions	621	593	73%
Municipal Affairs	973	962	81%
Office of the Premier	3,224	3,195	93%
Public Safety and Solicitor General	6,367	6,402	93%
Social Development and Poverty Reduction	4,604	4,611	91%
Tourism, Arts, Culture and Sport	768	748	78%
Transportation and Infrastructure	1,748	1,735	92%