STATUTORY REVIEW OF THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

# General briefing for the Special Committee to Review the Freedom of Information and Protection of Privacy Act

January 2022

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

# TABLE OF CONTENTS

## PREFACE

The general briefing that follows is intended to provide the Special Committee to Review the Freedom of Information and Protection of Privacy Act with a foundation as it considers recommendations for BC's public sector access and privacy law. It will be supplemented by a more detailed and targeted package of recommendations that will be submitted later during your consultations.

The review process, mandated by FIPPA every six years, is necessary to ensure that the legislation continues to achieve its purposes in a changing information landscape. FIPPA impacts every British Columbian, and the statutory review provides an important opportunity for the public and stakeholders to bring their concerns and recommendations forward.

Although the legislation has recently been updated, the work of the Special Committee is no less important. Several recent amendments to FIPPA addressed earlier recommendations made by my office and by the last Special Committee, but work remains. Some of the earlier recommendations not addressed by the recent amendments continue to have merit, and other developments in law and technology deserve your consideration to ensure that FIPPA continues to achieve its purposes in the years to come.

My office looks forward to supporting the Special Committee's work and to assist in realizing the recommendations that result from its work.

January 31, 2022

**ORIGINAL SIGNED BY**

Michael McEvoy
Information and Privacy Commissioner
for British Columbia

# INTRODUCTION

Since enactment of the *Freedom of Information and Protection of Privacy Act* (FIPPA) almost thirty years ago, British Columbians have had both a right of access to information in the custody and under the control of public bodies and protections for their privacy.

Those three decades have brought significant shifts in the information and technology landscape, with profound effects on both access to information and on privacy.

When the legislation was passed in 1992, public bodies worked predominantly with hard copy records. This is reflected in the definition of "record" in the Act, which starts by listing books, documents, maps, drawings and letters, and other traditional forms of records. These traditional record types, especially paper-based files, allowed for easier processing of access requests as staff dealt with a more finite range of materials, making the retrieval and review of records more straight-forward.

We are long past the time when responsive records can simply be pulled from a filing cabinet. Public bodies now deal with a greater diversity of record types, and varied ways in how these records are used and stored. The responsibility has also shifted to where, in the age of email, every public body employee is to a large degree responsible for managing their own emails.

The increasing magnitude and diversity of information collected by public bodies has assisted them to both serve the public and develop a greater understanding of issues they face in decision making. At the same time this has presented challenges to ensuring a full and accurate capture and preservation of records, key to both public body operations and to the right of access. This has made the process of responding to requests more complex.

These challenges, along with other processing concerns that my office investigates, come at a time when the demand for information is on the rise. Public sector information has real value for people, communities, and organizations. Information obtained through an access to information request or proactive disclosure can be used to understand and engage in policy making, drive product development and innovation, and better understand what is happening in our communities.

This demand for information has never been more apparent than during the ongoing pandemic. Access to government data has been a heavily debated topic, as citizens seek to better understand the threats they face, and the efficacy of public health responses. The importance of transparency in a time where government must make difficult decisions that affect how we go about our lives cannot be overstated.

While public bodies are creating and using more records, the public's right of access to them has been narrowed. The information that can be withheld under the exceptions to disclosure has widened, as has the number and types of records that are exempt from access requests all

together. In other words, the increased ability of public sector bodies to create and collect information, about us and about our communities, has not been balanced with similar progress on our right of access. In fact, the opposite has occurred, which has the effect of limiting the transparency and accountability FIPPA is meant to provide. This is a matter in which the Special Committee must seek to realign matters so that the legislation meets public needs and expectations.

The decades since FIPPA's enactment have also seen great changes in the policy environment for privacy.

Part of the drive for modern privacy laws was the development of computing and automation to store and process personal information. As the ability of organizations to collect and store information about individuals increased, governments introduced laws based on common privacy principles and established oversight regimes to uphold and enforce those laws.

Today, of course, computing power has increased exponentially. There is more information about us, and more of an ability to combine and analyze that data for new purposes. This increase in technological capacity has been supported by a steady increase in the legal authorities in FIPPA that allow public bodies to process personal information.

And while the ability and authority for public bodies to process personal information has greatly increased, the protections around those activities are only beginning to catch up.

Public sector bodies need our personal information to do their work and FIPPA provides for this in several ways. The increase in processing power and legal authorities for public bodies can result in insights and improved services, but it comes at a risk for individuals' privacy. The privacy rules and obligations in FIPPA, along with the oversight powers given to my office, need to account for and keep up with technological advances that allow for greater collection, use and disclosure of our personal information. Clear and up-to-date privacy rules will result in establishing guardrails for public bodies' use of new technologies. The ultimate result will be public trust and confidence in the actions of our public institutions.

# LEGISLATION

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

The purposes of the legislation are to make public bodies more accountable to the public by providing a right of access to records, including to an individual's own personal information, and by specifying limited exceptions to that right. The Act is also meant to protect personal privacy by setting out rules around the collection, use and disclosure of personal information. To ensure that these purposes are achieved, the legislation also provides for independent oversight of decisions made under the Act.

## *Information rights*

An applicant who makes a request has a right of access to records that are in the custody and under the control of public bodies, including to records containing personal information about themselves.

This right makes public bodies more accountable to the public by making their actions and decision-making more transparent. This in turn allows the public to better understand and scrutinize what is happening in the public sector. Individuals can seek records about what is happening in their community, the use of their tax dollars, and decisions made about their health care.

These benefits are neatly summarized in an oft-quoted citation from the Supreme Court of Canada. In a judgment going back 25 years, the Court held that "The overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry."[1]

Anyone can make an access request. FIPPA requires public bodies to assist applicants and sets out the manner and timeline for responding to requests. For example, public bodies must conduct an adequate search for records and respond to a request not later than 30 business days after its receipt (unless the Act allows them to take a time extension).

Access requests can be subject to fees, both for making a request and for certain tasks associated with locating and producing records. Except for the new application fee, the fees charged to applicants can be excused by public bodies when the applicant cannot afford payment, it is for any other reason fair to excuse payment, or when the record relates to a matter of public interest.

The right of access to records is to some extent limited by exclusion of some record types, such as records that are available for purchase and certain forms of meta-data. A further limit is the ability, sometimes the duty, of public bodies to refuse access under a disclosure exception. Some of these exceptions are mandatory, such as cabinet confidences and information that could be harmful to business interests of a third party or personal privacy. Where one of these applies, a public body must refuse to disclose the protected information. Other exceptions, such as those for policy advice or solicitor client privilege, are discretionary. Both types of exceptions are meant to balance the right of access with the need to protect certain information from disclosure.

Of course, nothing in FIPPA prevents public bodies from proactively disclosing records and information that do not contain personal information. Making information and records more

[1] *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC), [1997] 2 SCR 403

readily available encourages civic engagement and public sector accountability without incurring the costs and delays that can accompany formal access requests.

However, FIPPA's requirements to proactively disclose information are limited. Amendments made in 2011 did require public bodies to establish one or more categories of records that are available to the public without a request. My office investigated how this requirement was being met and offered feedback on those efforts in a report released in 2020.[2]

There are also cases where a public body must disclose, without delay, information to the public or an affected group of people or applicant. This is triggered when the information is about a risk of significant harm to the environment or to the health and safety of the public or a group of people; or that, for any other reason, is clearly in the public interest. These mandatory disclosures override any other provisions in FIPPA, including the disclosure exceptions mentioned above. My office has provided guidance to public bodies on this requirement, conducted investigations into whether information should have been disclosed under this section, and, where appropriate, ordered such disclosures.[3]

### *Protection of Privacy*

FIPPA sets out rules for the collection, use and disclosure of "personal information." A key principle is that a public body cannot collect, use or disclose personal information unless FIPPA authorizes it. An example is the authority to collect personal information that "relates directly to and is necessary for a program or activity" of the public body. Another example is the authority to collect personal information where an enactment allows it.

A measure of transparency is found in the requirement that a public body must, in most cases, notify individuals about the purpose for which their personal information is collected.

Public bodies are also required to provide reasonable safeguards for personal information in their custody or under their control. These safeguards are generally considered to be administrative, physical, and technical in nature. Factors such as the sensitivity of personal information and the potential for harm will influence the nature and extent of the safeguards in each case.

Other privacy protections include the duty to conduct privacy impact assessment (PIAs) to determine whether proposed initiatives comply with the law. My office regularly reviews PIAs submitted by public bodies seeking comment on the privacy implications of proposed projects or systems.

A welcome development in the recent amendments to FIPPA is the new requirement to notify affected individuals of certain privacy breaches, and the duty for public bodies to develop

[2] Investigation Report 20-01 https://www.oipc.bc.ca/investigation-reports/3432
[3] Investigation Report F16-02 https://www.oipc.bc.ca/investigation-reports/1972

privacy management programs.[4] These new requirements will better position public bodies to manage and safeguard our personal information.

## THE WORK OF THE OIPC

The Commissioner is responsible for monitoring how the Act is administered to ensure that its purposes are achieved. While oversight provided under the Act is broad and effective, some improvements can be made to strengthen and update the Commissioner's oversight powers.

Much of our work involves responding to requests to review decisions made by public bodies under FIPPA, particularly decisions to withhold information. We also investigate complaints about public bodies' handling of personal information.

While the above functions are responsive in nature, I am also empowered to undertake investigations and audits on my own motion, to engage in research, to inform the public about the Act, and to comment on different types of initiatives. The ability to investigate and proactively engage with access and privacy issues is part of a modern regulatory approach, and one that can be further expanded through legislative reform.

My office's oversight powers have remained largely unchanged despite the increasing complexity of the issues we encounter. The automated processing of personal data, big data analytics, and other technological developments were not part of the environment faced by legislators when they approved FIPPA in 1992. To address these matters, we will be bringing forward recommendations that would improve and streamline our own processes, while also providing stronger and more effective oversight related to technology changes.

### Requests for review and access complaints

Applicants can ask us to review a public body's decision to withhold information, to ensure that redactions are lawful. They can also complain about other issues in the handling of their request, such as whether an adequate search for records was conducted or whether a fee charged was appropriate.

In the last fiscal year, my office received approximately 885 requests for review and complaints about access requests.

OIPC investigators attempt to resolve requests for review and complaints informally, either by working with all parties to achieve consensus about the disposition of a file or by issuing findings. It can be challenging to mediate these issues, especially given that parties may appear

[4] What this entails will be established through directions to be issued by the Minister, but my office has outlined the key components of such programs in our last submission to the Special Committee that reviewed FIPPA and in guidance on Accountable Privacy Management in BC's Public Sector: https://www.oipc.bc.ca/guidance-documents/1545

in our office because their relationship is strained. Yet our skilled case review and investigator teams are able to resolve the vast majority of these files without a formal appeal hearing and binding order. Those that are not resolved, which typically include complex and contentious matters, proceed to adjudication.

Our own accountability is assured through judicial review by the Supreme Court of British Columbia.

## Privacy Complaints

OIPC investigators also look into privacy complaints, typically about whether a public body lawfully collected, used or disclosed a complainant's personal information. They will generally make a finding as to what occurred and whether what occurred complied with the law. This gives the opportunity for individuals' concerns to be heard, and for the public body to take corrective action, when needed.

In the last fiscal year, the OIPC investigated 81 privacy complaints about public bodies.

## Orders

The OIPC resolves most requests for review and complaints through the investigation and mediation process. However, a small percentage proceed to inquiry where an adjudicator decides the application of FIPPA and issues a binding order.

The OIPC's adjudicators issued 60 orders in the last fiscal year under FIPPA. A few are cited below to give a sense of the issues encountered and their resolution through adjudication.

### *Order F19-36*

An applicant requested records from the District of Sechelt related to a residential property development where geological issues resulted in multiple lawsuits. The disputed records consisted of numerous emails.

The adjudicator concluded that solicitor client privilege applied to some of the records, along with some information determined to be an unreasonable invasion of third party's personal privacy. The District was permitted to withhold that information. However, the adjudicator ordered the rest disclosed to the applicant.

The District petitioned the BC Supreme Court to judicially review the adjudicator's decision. The Court dismissed the petition leaving the adjudicator's order in place.

### *Order F20-50*

Two applicants made separate requests to the Ministry of Forests, Lands, Natural Resource Operations and Rural Development for access to information related to human remains discovered in a park located on the land of a traditional Lheidli T'enneh village and burial ground.

The Ministry refused to disclose the responsive records in part because they said doing so would result in numerous harms.

The adjudicator found that disclosure of the sought-after information would disrespect Lheidli T'enneh's express wishes and publicly portray the sensitive and sacred nature of the disputed information in a manner that is disrespectful to Lheidli T'enneh. The adjudicator also determined that the Ministry could refuse to disclose the information at issue because it could reasonably be expected to harm relations between it and an Indigenous governing entity.

### *Order F20-57*

Three Indigenous governments argued that the Ministry of Health was required to disclose information, including personal information, related to COVID-19 and its transmission in their communities. Section 25 of FIPPA requires a public body to, "without delay, disclose to the public, to an affected group of people or to an applicant...information about a risk of significant harm to the environment or to the health or safety of the public or a group of people."

The Ministry of Health argued that that *Public Health Act* emergency powers override its duty of public interest disclosure. I rejected this argument but determined on the facts of the case that s. 25 did not require the Ministry to proactively release the requested information, as sufficient information was available at the time for the complainants and to the public to take steps to avoid or mitigate risks connected with COVID-19.

## Privacy breach investigations

The OIPC received 92 voluntary FIPPA privacy breach reports in the last fiscal year. This process allows the OIPC to provide advice and guidance to public bodies in their breach response, helps to ensure that citizens have the information they need to better protect themselves from the consequences of a breach, and contributes to our understanding about the cause of breaches and how they can be prevented.

With the new requirement for mandatory breach reporting by public bodies, the number of breach reports submitted to my office is expected to rise, and this is something we are actively preparing for.

## Recent public sector reports

As noted earlier, our office has long used the own-motion investigation and audit powers under FIPPA to examine leading issues, always with a view to supporting better access and privacy practices across our public sector, as the following sample of recent reports illustrates.

*Section 71: Categories of records available without a request (June 2020)*

This investigation surveyed 30 public bodies to determine compliance with the requirement in s. 71 of FIPPA to establish categories of records available without an access to information request. The investigation found that the approach public bodies took to complying with this section of FIPPA was often inconsistent. The report outlines these different approaches and highlights key criteria for public bodies to meet their responsibility under this section.

*Now is the time: A report card on government's access to information timeliness (September 2020)*

This was the latest special report in our series on the timeliness of government's responses to access to information requests. While response times improved since our last report in 2017, government failed to comply with FIPPA's legislated timelines in thousands of cases.

*Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector (June 2021)*

This joint report with the BC Ombudsperson and Yukon Ombudsperson and Information and Privacy Commissioner looked at the challenges of fairness and privacy arising from the use of artificial intelligence, or AI, in the public sector. The report explores the regulatory challenges that come with new and intricate technologies and provides some best practices and general guidance for public bodies when implementing AI.

The report includes several recommendations, including committing to the principles of transparency, accountability, legality, procedural fairness and protection of privacy, as well as a practice of notifying an individual when an AI system is used to make a decision about them.

*The impact of COVID-19 on access to information (December 2021)*

This report considered how public bodies on the front line of the pandemic responded to an increase in access requests while at the same time managing their own workplace disruptions.

As noted earlier, FIPPA provides some relief to public bodies in meeting timelines when faced with challenging circumstances, and this, along with other steps taken by the public bodies surveyed, proved to be useful. The public bodies we surveyed reported that the increased attention on the demand for records and information, as well as new processes they had put in place, should give further support to their access to information work going forward.

The report also comments on the ongoing debate around the proactive disclosure of COVID-19 data, and the importance of transparency in the public health response.

## Audit and Compliance Program

The OIPC's Audit and Systemic Review team is responsible for conducting audits and systemic investigations of public bodies and organizations either in response to a complaint, or proactively. Audits and systemic investigations result in a public report, and they typically include recommendations.

Past audits of public bodies have focused on their access to information processes, privacy breach management, and an examination of the Insurance Corporation of BC's information sharing agreements.

## Guidance and outreach

Often the OIPC is consulted directly by public bodies seeking our comment on proposed initiatives or questions. When this occurs, we respond to and work directly with those public bodies. It is far better to address and resolve potential issues up front. This avoids the need for costly program changes or future regulatory action.

We also focus on releasing guidance documents for the public and for public bodies about the legislation and other relevant access and privacy issues. It is important that citizens understand their right of access and how their privacy is protected, and for public bodies to have access to the best practices and expectations for upholding their responsibilities.

FIPPA related guidance materials released since the last statutory review are set out in Appendix A.

In addition to offering guidance materials, we meet with stakeholders and make presentations. In the last fiscal year, OIPC staff held numerous meetings with public bodies and made 40 speaking presentations.

## Inter-jurisdictional collaboration

The OIPC works with our counterparts across the country and internationally to advance our knowledge and expertise in access and privacy issues, improve regulatory performance, and collaborate on joint initiatives.

Each year, Canada's federal, provincial, and territorial information and privacy oversight agencies meet to share our experiences and priorities, and to discuss issues of joint concern. We typically also issue a communique at the conclusion of the meeting, advising the public of our common position with respect to immediate challenges in a priority area.

Some of the more recent work includes the following.

*Joint Statement by Federal, Provincial and Territorial Privacy Commissioners on Privacy and COVID-19 Vaccine Passports*

In May 2021, we released a joint resolution and statement on the issue of vaccine passports with our federal, provincial and territorial counterparts. The resolution stated that passports could be a useful tool to allow people to travel and gather, and could support economic recovery while protecting public health. However, the joint statement outlined the necessity of adhering to fundamental privacy principles in the development of vaccine passports to ensure compliance with applicable privacy laws. This included incorporating best practices to achieve the highest level of privacy protection commensurate with the sensitivity of the personal health information that would be collected, used, or disclosed.

*Consultation on privacy guidance on facial recognition for police agencies*

In 2021, we jointly developed guidance with other privacy protection authorities on facial recognition for police agencies. The guidance is intended to clarify privacy obligations with a view to ensuring any use of facial recognition complies with the law, minimizes privacy risks, and respects privacy rights.

The draft guidance was sent out for stakeholder feedback in June 2021. In BC, we reached out to BC police services to gather feedback on whether the guidance can be practically implemented, whether it will have the intended effect of ensuring police agencies' use of FRT is lawful while mitigating privacy risks, and the potential for negative consequences arising from the recommendations. The federal office is currently updating the guidance based on stakeholder feedback, and we will publish the guidance on our website upon completion.

*Federal, Provincial and Territorial Information and Privacy Commissioners and Ombudsman Issue Joint Resolution About Privacy and Access to Information Rights During and After a Pandemic*

In June 2021, we released a joint resolution and statement with federal, provincial, and territorial counterparts to call on governments to use the lessons learned from the COVID-19 pandemic to improve privacy and access to information rights. The pandemic accelerated longstanding concerns about increasing surveillance by public bodies and private corporations and the slowing down of access requests. It has also highlighted the need to modernize the access to information system by leveraging technology and innovation to advance transparency.

The joint resolution adopted 11 access to information and privacy principles and called on Canada's governments to show leadership by implementing them and making the modernization of legislative and governance regimes about freedom of information and protection of privacy a priority.

## International work and collaboration

The fact that data flows ubiquitously across all borders means regulators of personal information must coordinate activities to properly serve and protect their citizens. The OIPC has been a leader both nationally and internationally in these matters. We head the Governing Council and Secretariat for the Asia Pacific Privacy Authorities (APPA) forum. This is a network of 19 regulators from around the Asia Pacific that meet twice a year to tackle issues of new technologies and the management of privacy enquiries and complaints. The term of the OIPC as Secretariat was recently renewed by APPA members and is set to run until the end of 2023.

We are responsible for chairing monthly conferences calls of Global Privacy Enforcement Network regulators based in the Asia Pacific region which focus on privacy enforcement issues, trends, and experiences among global regulators.

# THE NEED FOR REFORM

## Previous Committees

FIPPA's drafters had the foresight to include a requirement for the statute's review every six years. These reviews are key to ensuring that the legislation remains fit for purpose.

Several recommendations made by the last Special Committee, in 2016, were addressed in the recent package of amendments to the Act, particularly those focusing on privacy and on increased penalties and offences. Appendix B to this submission is a table showing the extent to which the 2021 amendments addressed the Special Committee's 2016 recommendations.

However, some of the recommendations made in 2016 that have not been adopted continue to merit your assessment. My office intends to highlight a number of those outstanding recommendations during your consultation process as I expect other presenters will do as well.

### *National trends*

Several Canadian jurisdictions have recently amended or reviewed their public sector access and privacy laws. These developments provide an opportunity to learn from what is occurring elsewhere and to improve our own legislation.

In the past few years, amendments to freedom of information and privacy legislation were brought forward in a number of provinces, including Manitoba, Ontario, Quebec, New Brunswick, Prince Edward Island, and Nova Scotia; as well as in all three territories.[5]

[5] Bill 49, *The Freedom of Information and Protection of Privacy Amendment Act, 2020*, 3rd Sess, 42nd Leg, Manitoba, 2020; *Data Integration Regulation,* Ontario Reg 185/2021; Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information, 2021,* 1st Sess, 42nd Leg, Quebec, 2021; Bill 76, *An Act to Amend the Right to Information and Protection of Privacy Act, 2021*, 1st Sess, 60th Leg, New Brunswick, 2021; Bill 39, *An Act to*

Amendments to the federal *Access to Information Act* were made in 2019, and that Act is currently under review.[6] A similar statutory review, of Newfoundland and Labrador's *Access to Information and Privacy Act*, was recently completed in that province.[7]

In some cases, the amendments to these laws added provisions that have long been included in our own legislation. For example, the federal *Access to Information Act* was recently amended to include order-making power for the federal Information Commissioner, something that has always existed in FIPPA. In another example, both the federal access law and the law in the Northwest Territories were updated to include a mandatory review clause, which again, is something that we already have here in BC.

In other cases, the amendments and recommendations made elsewhere offer a way forward. For example, the federal Privacy Commissioner has recommended that the *Privacy Act* be amended to require government to consult with his office about legislation that has privacy implications. This kind of requirement, which already exists in Newfoundland and Labrador's privacy and access law, is well suited to our situation here in British Columbia.

Another area where we can learn from other jurisdictions is the use of automated decision-making. These systems use automated processes to analyze and make inferences from large amounts of data. While these processes can offer powerful tools for research and analysis, they also raise privacy concerns, particularly when they are used to make a decision that affects an individual. Several jurisdictions have put forward ideas to regulate the use of this kind of technology. For example, Europe's *General Data Protection Regulation* gives individuals the right to object to profiling and automated decision making that has a legal or other significant effect on them.

Closer to home, both the Office of the Privacy Commissioner of Canada's submission[8] to the Minister of Justice and Attorney General of Canada on the modernization of the *Privacy Act*,

---

*Amend the Freedom of Information and Protection of Privacy Act*, *2018,* 3rd Sess, 65th Leg, Prince Edward Island, 2018; Bill 106, *Freedom of Information and Protection of Privacy Act (amended), 2021, 3rd Sess, 63rd Leg,* Nova Scotia, 2021, (passed first reading 12 April, 2021); Bill 24, *Access to Information and Protection of Privacy Act, 2018,* 2nd Sess, 34th Leg, Yukon, 2018; Bill 29, *An Act to Amend the Access to Information and Protection of Privacy Act, 2018*, 3rd Sess, 18th Leg, North West Territories, 2018; Bill 67, *An Act to Amend the Access to Information and Protection of Privacy Act, 2021*, 2nd Sess, 5th Leg, Nunavut, 2021.

[6] *An Act to amend the Access to Information Act and the Privacy Act and to make consequential amendments to other Acts*, SC, 2019, c. 18; Canada, Treasury Board Secretariat, *Reviewing access to information,* https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/reviewing-access-information.html

[7] Newfoundland and Labrador, *Access to Information and Protection of Privacy Statutory Review Committee 2020,* https://www.nlatippareview.ca/

[8] Office of the Privacy Commissioner of Canada. Submission of the Office of the Privacy Commissioner of Canada to the Minister of Justice and Attorney General of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_jus_pa_2103/#fn44-rf

and the *Newfoundland Access to Information and Protection of Privacy Act*, 2020 Statutory Review Committee[9] each made detailed recommendations on this topic.

As noted earlier, my office has also sought to understand the implications of automated decision making and other forms of artificial intelligence in a report co-authored with the Ombudsperson of BC and our colleague in the Yukon. That report, *Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector*, makes its own recommendations for legislative reform.

## CONCLUSION

I will provide a full set of recommendations for amendments in the coming months that focus on strengthening the Act, to ensure it is able to achieve its purposes now and in the years to come.

The recent changes to the legislation made improvements to privacy and to the penalties and offence provisions in the Act, but did not move the legislation forward when it comes to openness and transparency. To strengthen the access side of the Act, we plan to bring forward recommendations to narrow the exceptions to disclosure and to expand coverage of the Act.

Likely the most debated change in the recent amendments was the addition of the potential for public bodies to charge an application fee. This was quickly adopted by the provincial government, and my office intends to study its impact on the exercise of citizens' right of access in the coming months.

With respect to the protection of citizen personal information, the recent package of amendments fulfilled several earlier recommendations of both this office and the last Special Committee. However, these changes need to be supplemented and reinforced by regulations setting out rules for data linking and the use of automated processing to make decisions using personal information. These rules should give greater certainty to public bodies as they seek to use these processes, while at the same time respecting the privacy of individuals.

The goal of this general briefing has been to underscore that much work remains to strengthen FIPPA in a manner that meets it original purpose while serving our citizens.

Your deliberations will be crucial to ensuring that British Columbia's freedom of information and privacy law are robust enough to cope with developments in technology, in public programs and services, and public expectations around transparency and accountability. We are hopeful that recommendations made by the Committee at the conclusion of this review will be taken up by government and result in amendments at the earliest opportunity.

[9] Newfoundland and Labrador, *Access to Information and Protection of Privacy Statutory Review Committee 2020,* https://www.nlatippareview.ca/

# APPENDIX A: DOCUMENTS SINCE THE LAST SPECIAL COMMITTEE

Privacy and the B.C Vaccine Card: FAQ (September 2021)
This guidance document explains how the BC Vaccine Card) and the Public Health Orders work together with the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA).

Common or Integrated Programs and Activities (March 2021)
This guidance document aims to help readers understand what constitutes a "common or integrated program or activity" under FIPPA and the obligations associated with them.

FIPPA and online learning during the COVID-19 pandemic (April 2020)
This guidance document provides recommended guidance for educators to help them choose online learning tools that comply with the requirements of FIPPA.

Guide to OIPC Processes (FIPPA) (February 2020)
This guidance document addresses the most common procedures that the Office of the Information and Privacy Commissioner uses under FIPPA.

Disclosure of personal information of individuals in crisis (September 2019)
This guidance document informs public bodies and private sector organizations about the circumstances under which they can disclose personal information of an individual to a third party without the individual's consent in emergency situations.

Section 25: The duty to warn and disclose (December 2018)
This guidance document explains section 25 of FIPPA, which requires public bodies to proactively disclose information if it is in the public interest.

Tip Sheet: 10 tips for public bodies managing requests for records (January 2018)
This document provides our top 10 tips to help public bodies meet the timelines and requirements for responding to requests for records under FIPPA.

Employee Privacy Rights (November 2017)
This guidance document discusses the privacy impacts of employee monitoring programs.

Guide to Using Overt Video Surveillance (October 2017)
This guidance document is for public bodies and organizations that are interested in using video surveillance in compliance with FIPPA and PIPA.

Tip Sheet: Requesting records from a public body or private organization (September 2017)
This is a guidance document with tips on how to access records from a public body or private organization.

Guidance Document: Information Sharing Agreements (September 2017)
This guidance document is for public bodies and organizations that are interested in sharing personal information. It describes information sharing and explains the role and value of information sharing agreements to ensure compliance with FIPPA and PIPA.

Guidelines for social media background checks (May 2017)
This is a guide for public bodies and organizations that use social media to search for information about prospective employees, volunteers, and candidates. These activities are subject to privacy provisions in FIPPA and PIPA.

Time extension guidelines for public bodies (July 2016)
This guidance document explains how public bodies can submit time extension requests under FIPPA.

# APPENDIX B: COMMITTEE'S RECOMMENDATIONS

| Recommendation | | Addressed in Bill 22 |
|---|---|---|
| **MAJOR RECOMMENDATIONS** | | |
| **Proactive Disclosure** | | |
| 1. | Initiate proactive disclosure strategies that reflect the principle that information that is in the public interest should be proactively disclosed, subject to certain limited and discretionary exceptions that are necessary for good governance and the protection of personal information. | |
| **Duty to Document** | | |
| 2. | Adopt a duty to document to demonstrate a commitment to public accountability, in order to preserve the historical legacy of government decisions, and as a key records management component of proactive disclosure programs. | |
| **Information Management in Government** | | |
| 3. | Make all obligations related to the entire life-cycle of government records part of a cohesive and robust information management scheme. | |
| 4. | Ensure that archiving is a high priority. | |
| **Data Sovereignty** | | |
| 5. | Retain the data sovereignty requirement in s. 30.1 of FIPPA | |
| **Application of FIPPA** | | |
| 6. | Extend the application of FIPPA to any board, committee, commissioner, panel, agency or corporation that is created or owned by a public body and all the members or officers of which are appointed or chosen by or under the authority of that public body. | ✓ |
| 7. | Consider designating all publicly-funded health care organizations as public bodies under FIPPA. | |
| **FOI Processes** | | |
| 8. | Reduce the timeline in which a public body must respond to an access request from 30 business days to 30 calendar days. | |
| 9. | Review other timelines established in FIPPA with a view to reducing them in order to promote the efficiency and timeliness of the FOI process. | |
| 10. | Amend section 4(1) of FIPPA to establish that an applicant who makes a formal access request has the right to anonymity. | |
| **Mandatory Breach Notification and Reporting** | | |

| | | |
|---|---|---|
| 11. | Add a mandatory breach notification and reporting framework to FIPPA that includes:<br>• a definition of a privacy breach;<br>• a requirement to notify individuals when their personal information is affected by a known or suspected breach, if the breach could reasonably be expected to cause significant harm to the individual;<br>• a requirement that a public body report to the Commissioner any breach involving personal information under the custody or control of that public body, if the breach or suspected breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals;<br>• a timing requirement that the process of notification and reporting must begin without unreasonable delay once a breach is discovered;<br>• authority for the Commissioner to order notification to an individual affected by a breach or the public; and<br>• a requirement that public bodies document privacy breaches and decisions about notification and reporting. | ✓ |
| **ACCESS** | | |
| **Duty to Assist** | | |
| 12. | Amend s. 6 of FIPPA to add a specific requirement for public bodies to make the contact information of the person responsible for ensuring compliance available to the public. | |
| **Cabinet Confidences** | | |
| 13. | Amend s. 12 of FIPPA to permit the Cabinet Secretary to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees where the Cabinet Secretary is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception. | |
| **Personal Privacy** | | |
| 14. | Consider initiating a review of whether a parent of a child who was in care should have access to personal information about their deceased child. | |
| **Policy Advice and Recommendations** | | |
| 15. | Amend s. 13(1) of FIPPA to clarify that the discretionary exception for “advice” or "recommendations” does not | |

| | | |
|---|---|---|
| | extend to facts upon which they are based; or for factual, investigative or background material; or for the assessment or analysis of such material; or for professional or technical opinions. | |
| **Legal Advice** | | |
| 16. | Amend s. 14 of FIPPA to make it a mandatory exception unless the public body is the client and can choose to waive privilege, or if the client is a third party, the client agrees to waive privilege. | |
| **Law Enforcement** | | |
| 17. | Consider whether an explicit reference to investigations that are within the mandate of a professional regulatory body should be added to the definition of "law enforcement" in Schedule 1 so that a professional regulatory body may refuse to disclose information that may harm an investigation. | |
| **Fees** | | |
| 18. | Review the Schedule of Fees with a view to ensuring that fees are not a barrier to individuals' right of access, and that they provide reasonable compensation for substantial costs incurred by public bodies in responding to complex requests. | |
| 19. | Amend s. 75 of FIPPA to provide an automatic fee waiver for applicants when a public body has failed to meet the statutory timeline for responding to access requests. | |
| 20. | Consider reducing or eliminating fees when records have been completely severed such that, in essence, there are no responsive records because none of the information the applicant is seeking is disclosed. | |
| 21. | Make fee waivers available as a matter of course, without the applicant having to make a specific request, when there is significant public interest in disclosure. | |
| **PRIVACY** | | |
| **Privacy Management Program** | | |
| 22. | Add to FIPPA a requirement that public bodies have a privacy management program that:<br>• designates one or more individuals to be responsible for ensuring that the public body complies with FIPPA;<br>• is tailored to the structure, scale, volume, and sensitivity of the personal information collected by the public body;<br>• includes policies and practices that are | ✓ |

| | | |
|---|---|---|
| | developed and followed so that the public body can meet its obligations under FIPPA, and makes policies publicly available;<br>• includes privacy training for employees of the public body;<br>• has a process to respond to complaints that may arise respecting the application of FIPPA; and<br>• is regularly monitored and updated. | |
| **Notification for Collection of Employee Information** | | |
| 23. | Amend FIPPA to permit a public body to not notify the employee that it is collecting their personal information, either indirectly or directly, for the purpose of managing or terminating the employment relationship, where it is reasonable to expect that doing so would compromise (a) the availability or the accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee. | |
| **Disclosure outside of Canada** | | |
| 24. | Amend s. 33.1(1) of FIPPA to permit public bodies to post non-statutory investigation or fact-finding reports on-line where the public interest in disclosure outweighs the privacy interests. | ✓ |
| **Disclosure for Planning or Evaluating a Public Body** | | |
| 25. | Amend s. 33.2(l) of FIPPA to permit only de-identified personal information to be disclosed for the purposes of planning or evaluating a program or activity of a public body. | |
| **Privacy Impact Assessments** | | |
| 26. | Amend s. 69 of FIPPA to clarify and strengthen requirements with respect to privacy impact assessments. | ✓ |
| **OVERSIGHT OF THE INFORMATION AND PRIVACY COMMISSIONER** | | |
| **Unauthorized Destruction of Records** | | |
| 27. | Amend s. 42 of FIPPA to expand the Information and Privacy Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records within public bodies. | |
| **Data-Linking Initiatives** | | |
| 28. | Amend the definition for "data-linking" in Schedule 1 of FIPPA to define data-linking as the linking or combining of | ✓ |

| | | |
|---|---|---|
| | datasets where the purpose of linking or combining the information is different from the original purpose for which the information in at least one of the datasets that was originally obtained or compiled, and any purposes consistent with that original purpose. | |
| 29. | Address the privacy risks associated with data-linking initiatives within the health sector in consultation with the Information and Privacy Commissioner. | |
| **Unitary Process** | | |
| 30. | Amend Parts 4 and 5 of FIPPA to combine the complaint process and the review and inquiry process into a unitary process for the Commissioner to investigate, review, mediate, inquire into and make orders about complaints respecting decisions under FIPPA or other allegations of non-compliance with FIPPA. | |
| **ENFORCEMENT OF FIPPA** | | |
| **Unauthorized Destruction of Documents** | | |
| 31. | Amend FIPPA to make the alteration, concealment, or destruction of records with the intention of denying access rights under FIPPA an offence under FIPPA. | ✓ |
| **Privacy Protection Offence** | | |
| 32. | Amend s. 74.1 of FIPPA to make the unauthorized collection, use, and disclosure of personal information in contravention of Part 3 of FIPPA an offence under FIPPA. | ✓ |
| **Penalties** | | |
| 33. | Increase the maximum amount of fines for general offences from $5000 to $10,000 and increase the amount of fines for privacy offences committed by individuals to up to $25,000. | ✓ |
| 34. | Institute a fine of up to $10,000 for the offence of destroying, altering, or concealing a record with the intention of denying access rights under FIPPA. | ✓ |
| **GENERAL** | | |
| **Correction** | | |
| 35. | Amend FIPPA to require public bodies to correct personal information at the request of an individual the information is about if there are reasonable grounds for the public body to do so. | |
| **Review of Provisions that Prevail over FIPPA** | | |
| 36. | Appoint a special committee to conduct a review of the existing overrides of FIPPA and make recommendations to the Legislative Assembly as to whether they should be amended or repealed. | |

| | | |
|---|---|---|
| **Sector-Specific Privacy Legislation** | | |
| 37. | Enact new stand-alone health information privacy law at the earliest opportunity. | |
| 38. | Consult with stakeholders in the education sector as to whether there is a need for special provisions in FIPPA that are tailored to the education sector. | |
| **Chief Privacy and Access Officer** | | |
| 39. | Establish the position of Chief Privacy and Access Officer within government. | |