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

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

March 2022
Michael McEvoy
Information and Privacy Commissioner
for British Columbia

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

TABLE OF CONTENTS

INTRODUCTION

British Columbia staked out a leadership position in access and privacy law 30 years ago with the introduction and approval of the *Freedom of Information and Protection of Privacy Act* (FIPPA). Much has changed since then.

The passage of time, numerous court decisions expanding exceptions to disclosure, and amendments taking certain records out of the legislation's purview have combined to weaken FIPPA. We can and must do better. Robust access to information and privacy laws, though at times an anathema to governments of all stripes, are nonetheless vital to the overall foundations of democracy. They go to the heart of shining sunlight on the activities of our public bodies and allow citizens to hold those bodies to account.

The recommendations contained in this submission are aimed at putting BC back on a road to a leadership role in access and privacy law. My views about recent amendments to FIPPA fashioned through Bill 22 are well known, and not repeated in this submission. I would add only that I will be carefully assessing the impact of those amendments, and in particular the effects of the imposition of the access to information fee by the provincial government. I expect to publicly report on the latter issue in the months to follow. The Special Committee, I expect will have its own views about the recent changes and whether they ought to be reconsidered.

What the impassioned debate around Bill 22 and many of the submissions made to the Special Committee demonstrate is that FIPPA deeply matters to British Columbians.

Some of the recommendations that follow focus on areas of longstanding concern and will be familiar to those that engage in or follow the statutory review process. Others address recent challenges including those posed by advances in technology.

Our recommendations are ordered into three parts. They are access and accountability, privacy protections, and oversight and enforcement. This reflects both the purposes and structure of the legislation. And while some of these areas are in more need of reform than others, they all need your attention.

Taken together, what we have provided the Special Committee is intended to bolster and expand our right of access, add privacy rules with respect to the use of new information processes and technologies, and ensure that my office has the tools it needs to be able to provide active and engaged oversight.

ACCESS AND ACCOUNTABILITY

The right of access to public body information is a critical element of our democratic system of governance. This more than ever is the case in the age of misinformation, disinformation, government accountability, and for the health of our democracy generally. I have publicly stated that recent changes to FIPPA were detrimental to this right. In addition to the creation of an application fee, which is a barrier to access for many, the changes increased the types of records that simply fall outside our right of access.

The timing of the Special Committee's appointment presents an opportunity to put matters back on the proverbial rails. The recommendations below seek to breathe additional life into the access provisions of FIPPA. This can be done, in part, by moving ahead with bringing the administrative functions of the Legislative Assembly under FIPPA, and by bringing greater precision to the legislation's exceptions to disclosure so that they reflect FIPPA's original intent.

Coverage of the Legislative Assembly

Issue

The definition of "public body" in Schedule 1 of FIPPA specifically excludes "the office of a person who is a member or officer of the Legislative Assembly." This has the practical effect of shielding the entirety of the Legislative Assembly from the application of FIPPA, including its administrative functions.

Discussion

In a 2019 letter to the Speaker, along with the Offices of the Merit Commissioner and Ombudsperson, my office recommended that FIPPA be amended to include the administrative functions of the Legislative Assembly. Such a change would be calibrated to not "impinge on its important work as the legislative branch of government" and "ensures the constituency work of Members of the Legislative Assembly is not affected." Oversight for FIPPA would remain with the OIPC as an independent Officer of the Legislature subject to judicial review by the courts.

In response to the letter, both the government and opposition house leaders publicly indicated their support for making the administrative functions of the Legislative Assembly subject to FIPPA.[1]

It is again important to emphasize that the proposed recommendations would only subject the administrative functions of the Assembly to oversight. The independence of the Legislative Assembly would remain intact and not be impacted. Indeed, there is precedent for this in our Alberta neighbor to the east, whose *Freedom of Information and Protection of Privacy Act*

[1] https://www.timescolonist.com/local-news/foi-whistleblower-protection-should-apply-to-legislature-staff-watchdogs-say-4669700

includes the "Legislative Assembly Office" in its definition of a "public body" but, similar to what recommend here, does not include "the office of the Speaker of the Legislative Assembly and the office of a Member of the Legislative Assembly."

Conclusion

Access to information serves the public interest by holding governments to account for their actions and decisions. This includes the expenditure of public funds. There is no reason why the Legislative Assembly should not, in respect of its administrative functions, be subject to the same transparency and accountability rules as the more than 2,900 public bodies across the province. The executive branch of government, all local governments, universities, schools and many other institutions, including independent Officers of the Legislature, have complied with the access to information rules in place for almost 30 years in British Columbia. It is time for the Legislative Assembly to adhere to the same standards.

Recommendation 1
Include the administrative functions of the Legislative Assembly as a public body under FIPPA in such a way that maintains the important role that constituency records and other records subject to parliamentary privilege play in our democratic process.

Public interest override of cabinet confidences

Issue

Section 12 is a mandatory exception to disclosure that applies to the substance of deliberations of the Executive Council or any of its committees. It leaves no room for the Executive Council to exercise discretion if they determine that the public interest in disclosing information outweighs the need to protect cabinet confidences.

Discussion

Cabinet secrecy is a time-limited but long-held tradition in parliamentary democracies that allows open discussion and deliberation by members of the Executive Council. Section 12(1) recognizes the importance of such deliberations by creating a mandatory exception for records:

> The head of a public body must refuse to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees, including any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees.

The above section does not apply to records that have been in existence for 15 or more years and other limited cases involving decisions that are public.

Across Canada and around the world,[2] a variety of approaches have been taken to protect cabinet confidences. For example, at the federal level, cabinet records are excluded in the *Access to Information Act* in their entirety. For their part, most provinces are in line with BC, opting instead for a mandatory exception to disclosure and not a blanket exclusion.

Newfoundland and Labrador is unique among Canadian jurisdictions, with a public interest override found within that province's cabinet confidences section that states:

> 27(3) Notwithstanding subsection (2), the Clerk of the Executive Council may disclose a cabinet record or information that would reveal the substance of deliberations of Cabinet where the Clerk is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception.

While it is true that the general public interest override found in s. 25 of FIPPA applies to records subject to s. 12, we are of the view that a provision similar to the one in Newfoundland and Labrador would be advisable for two reasons. First, the threshold for the public interest override found in s. 25, "clearly in the public interest," is very high and requires an immediate disclosure of the information in question. In other words, it requires the proactive disclosure of information outside the FOI process. Second, we are of the view that given the special nature of cabinet confidences, the decision-maker in question for release should actually be cabinet itself and not the head of the public body in question.

There is some precedent for this in s. 16 of FIPPA, where the head of a public body must not disclose information which could reasonably be expected to harm inter-governmental relations or negotiations unless the Executive Council consents to the disclosure.

Previous recommendations

This issue was considered by both the 2010 and 2016 Special Committees. The 2010 Committee noted requests to amend s. 12, but concluded that it was undesirable to make confidential records more accessible at that time.

The 2016 Committee took a different approach. In their report, they recommended that FIPPA be amended to:

> [P]ermit 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.

[2] Stanley L. Tromp, *Fallen Behind: Canada's Access to Information Act in the World Context*, 2nd ed (Vancouver: BC Freedom of Information and Privacy Association, 2020) at ch 2.

Conclusion

Adding flexibility to an otherwise mandatory exception allows for the disclosure of cabinet information when the Executive Council determines that doing so is in the public interest.

Recommendation 2
Amend FIPPA to allow the Executive Council to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees when they are satisfied that the public interest in the disclosure outweighs the need to protect cabinet confidences.

Restoring section 13 to its intended purpose

Issue

Section 13 of FIPPA allows public bodies to withhold information that would reveal "policy advice or recommendations." Over time, in response to public body arguments and court decisions, this provision has been interpreted in a manner that has eroded the public's right of access.

Discussion

Section 13(1) rightly protects "advice or recommendations developed by or for a public body or a minister." Its purpose is to provide for the full and frank discussion of advice or recommendations within the public service.

However, a 2002 decision of the British Columbia Court of Appeal gave what has long been seen as an overly broad interpretation to the phrase "advice or recommendations." This prompted considerable criticism, and the Ontario Court of Appeal later explicitly declined to adopt that interpretation in relation to the same wording in Ontario's *Freedom of Information and Protection of Privacy Act*.

The situation was worsened by two British Columbia Supreme Court trial decisions in 2013 that extended the concept of "advice or recommendations" to include *factual information* compiled and selected by an expert using their expertise, judgment and skill to provide explanations necessary to a public body's deliberative process. This was based in part on what we respectfully submit was a misreading of the 2002 British Columbia Court of Appeal decision.

Taken together these decisions represent, and again with respect and deference to the courts, an expansion of the concept of "advice or recommendations" beyond what the Legislature intended. As an example, s. 13(2)(a) provides that a public body "must not refuse to disclose" as "advice or recommendations" any "factual material." Reading "advice or recommendations" to

include "factual information" that an expert has compiled ignores FIPPA's express language and the Legislature's unambiguous intent. It is no wonder that the Supreme Court of Canada has cast serious doubt on the correctness of these trial court decisions in *John Doe v. Ontario (Finance)*.[3]

The grave implications of the 2013 decisions can be illustrated by a simple example. Suppose a scientist is retained by a health authority to provide their expert recommendations on how to address a public health risk. Relying on their expertise, they gather data from relevant sources. They analyse that information and, in their report, make several recommendations to the health authority. The health authority announces public health measures based on the report and recommendations but does not disclose the report. A formal access request is later made, and the health authority withholds both the recommendations and the compiled data. In the latter case, it argues that the pre-existing data is "factual information" compiled by an expert and therefore is itself protected "advice or recommendations," despite s. 13(2)(a). This prevents the public and public health experts from understanding the factual basis for the analysis, for the recommendations flowing from the analysis, and for the public health measures. This outcome, which flies in the face of the express language and clear legislative intent of s. 13(2)(a), is enabled by the 2013 decisions.

Previous recommendations

Our office recommended changes to this section to the 2004, 2010, and 2016 Special Committees to Review FIPPA.

The 2004 and 2016 Special Committees[4] recommended amending s. 13(1) to clarify that the discretionary exception for "advice" or "recommendations' does not extend to:

- facts upon which they are based;
- factual investigative or background material;
- the assessment or analysis of such material; or
- professional or technical opinions.

[3] 2014 SCC 36 (CanLII). To give only one example, at paragraph 30 of the decision, the Court noted that the Ontario legislation excluded, like British Columbia's Act, "factual information," which the Court characterized as "objective information," describing it as one of two categories of exclusion, under section 13(2), from the concept of "advice or recommendations." The Supreme Court's observation underscores the air of unreality shot through the British Columbia Supreme Court's creation of a new class of protected "factual information" despite the explicit language of section 13(2)(a).

[4] The 2010 Committee ultimately did not endorse the recommendations of this office or the 2004 Committee, concluding instead that keeping the advice exception was prudent for evidence-based interpretations, analysis and recommendations.

Conclusion

It is well past time for government to—after repeated calls for reform by previous Special Committees of the Legislative Assembly, by this office, and by many others—return s. 13(1) to its original intent. Doing so would in no way impair the ability of public servants to continue to confidentially formulate frank advice and recommendations for government, which is what the Legislature intended to enable, and no more.

Recommendation 3
Amend s. 13(1) of FIPPA to clarify the following: • "advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process, and to that extent, are similar concepts and often interchangeably used terms; • "advice" or "recommendations" does not apply to the facts upon which the advice or recommendation is based; and • "advice" or "recommendations" does not apply to factual, investigative, or background material, for the assessment or analysis of such material, or for professional or technical opinions.

Ensuring FIPPA remains a complete code

Issue

Section 14 of FIPPA allows a public body to refuse to disclose information that is subject to solicitor client privilege. In *Richmond (City) v. Campbell*, 2017 BCSC 331, a judicial review of an order of this office, the BC Supreme Court held that while the wording of s. 14 does not include settlement privilege, the fact that FIPPA does not contain a clear and specific abrogation of common law settlement privilege means a public body is still entitled to rely on it to refuse disclosure.

We say, with respect, that this overrides the Legislature's intended purpose of making FIPPA a complete set of rules for the public's right of access to information. Section 2(1)(c) of FIPPA states that FIPPA achieves its stated purpose in part by "specifying limited exceptions to the rights of access". The *Campbell* decision adds an additional exemption not found anywhere in the statute. As a result, information that was previously released, such as severance amounts paid by public bodies, is now being withheld from disclosure.

Discussion

FIPPA is a complete code. No common law and other legal rights that would otherwise render certain information confidential or privileged—such as non-disclosure provisions or contract pricing—were ever intended to exist inside of its statutory provisions. The exceptions reflect a careful balancing of multiple interests while promoting the transparency required of public bodies. Had the legislature intended to include settlement privilege, it could have done so as is the case in Alberta.[5] The entirely new exception created by the *Campbell* decision does not reflect that careful balance and is a step backwards for transparency.

Specific details of settlement agreements with public bodies should not remain under a cloak of secrecy. Scrutiny of legal disputes and settlement amounts is essential for the public to be able to assess public bodies' actions. These settlements often involve significant expenditures of funds. The protections afforded by existing exceptions adequately protect any interests that may be impacted by the general release of this kind of information, including privacy concerns. In fact, this had been the case for nearly 20 years before the *Campbell* decision.

Conclusion

FIPPA was intended to be a complete code for what exceptions apply to records in the custody or under the control of public bodies, and the limits on the public right of access should not extend beyond what the statute provides.

Recommendation 4
Clarify the language in s. 2 to specifically state that despite any common law or legal exemption to disclosure, public bodies may only rely on the specific exceptions contained in FIPPA.

Harmonization of the correction threshold in FIPPA with PIPA

Issue

FIPPA does not clearly set out when public bodies are required to correct personal information. This results in uncertainty for the individuals when trying to correct inaccurate or incomplete information.

[5] Section 27(1) of the *Freedom of Information and Protection of Privacy Act*, RSA 200, F-25 states that a public body may rely on "any type of privilege."

Discussion

FIPPA requires that public bodies keep information accurate and complete. Section 29 also contains the right for individuals to request that their personal information be corrected, but does not identify when a public body is required to actually make the correction.

By contrast, BC's private sector *Personal Information Protection Act* (PIPA) requires organizations to correct personal information in response to a request to do so when "the organization is satisfied on reasonable grounds that a request made [to correct personal information] should be implemented."[6]

Previous recommendations

The 2016 Special Committee to Review FIPPA adopted our earlier recommendation on this topic, which is again repeated in this submission.

Conclusion

There is no clear reason why the correction provisions of PIPA and FIPPA are different, and it is in the public interest to strengthen the right to correction found in FIPPA to the level found in PIPA.

Recommendation 5
Add to s. 29 of FIPPA a requirement that public bodies correct personal information when an individual requests that their personal information be corrected - if the public body is satisfied on reasonable grounds that the request made should be implemented.

Measures to support the management of public body records

Issue

A meaningful right of access depends on public bodies establishing robust information management systems. If records are not created or properly retained, or if they cannot be located and retrieved, this right and its underlying objective of public sector accountability is fundamentally impaired.

Discussion

There is very little in FIPPA now that addresses this foundational matter and certainly nothing on the statute books that provides any independent oversight of government's management of record systems.

[6] Section 24(2).

As it presently stands, FIPPA requires public bodies to retain an individual's personal information for a year—if the information is used to make a decision that directly affects the individual. This gives the affected individual a reasonable opportunity to obtain access to that information.

FIPPA was also just amended to make it an offence to destroy or alter a record to avoid complying with a request for access.
These provisions, while helpful, do not go anywhere near far enough. This combined with the lack of independent oversight of the government's *Information Management Act,*[7] serve to undermine public trust and confidence in the Province's record management systems.

In contrast, Ontario's *Freedom of Information and Protection of Privacy Act* contains a provision that requires public sector institutions to have record keeping and retention rules and policies.

This kind of provision in FIPPA would benefit British Columbians by combining a requirement for all public bodies to keep proper record systems along with independent oversight of these obligations to make sure they happen.

That oversight responsibility should also include the authority for the Office to review matters or allegations of unauthorized destruction of records set out in any enactment or other legal instrument of a local public body. This would cover allegations of the unauthorized destruction of records that occurs outside of, or prior to, an access request for them. This kind of oversight power has long existed in Alberta.[8]

Previous recommendations

Our office has previously recommended both the addition of a duty to document to FIPPA and oversight over allegations of the unauthorized destruction of records.

Both recommendations were supported by the 2016 Special Committee.

Conclusion

The records management provisions that exist in Ontario and Alberta's public sector access and privacy laws should be incorporated into FIPPA. This will strengthen access to information by helping to ensure that records are properly managed by public bodies, as per their own rules and requirements.

---

[7] SBC 2015, c 27. This is standalone legislation that is the government's primary information management law. It applies primarily to core government ministries and limited other public entities and is overseen by a Chief Records Officer who reports to the Minister.

[8] *Freedom of Information and Protection of Privacy Act*., RSA 2000, c F-25, s. 53(1)(a).

Recommendation 6
Amend FIPPA to require that public bodies have in place reasonable measures respecting records management.

Recommendation 7
Amend s. 42 of FIPPA to expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records. The Commissioner should have jurisdiction over the unauthorized destruction of records as set out in: • any enactment of British Columbia, or • set out in a bylaw, resolution or other legal instrument by which a local public body acts or, if a local public body does not have a bylaw, resolution or other legal instrument setting out rules related to the destruction of records, as authorized by the governing body of a local public body. Introduce offenses and penalties tied the above obligations.

PROTECTION OF PRIVACY

Public bodies have a very serious responsibility to properly use and protect the personal information they collect from us. This obligation has become more challenging over time. New technologies and processes have expanded the ability of public bodies to make use of our data, which has in turn placed pressure on legislators to ensure FIPPA keeps pace with these advances.

Many of the recent Bill 22 amendments focused on addressing this balance, as it sought to provide greater allowance for public bodies to use foreign service providers for storing personal information, and to strengthen or add requirements for privacy impact assessments and privacy management programs.

The recommendations below also seek to get at the issue of how public bodies can engage new technologies and data processing within a set of rules that allow for the proper protection of our personal information.

Clarifying that privacy protections apply to teaching and research materials

Issue

Section 3(3)(i) seeks to protect the intellectual property of faculty members, teaching or research assistants, or other people carrying out research at post-secondary educational bodies. However, as written, the provision appears to omit privacy protections for research subjects or for anyone whose personal information is included in teaching or research material.

Discussion

This shortcoming was pointed out by the very first Special Committee to review FIPPA in 1999, which recommended that the statute be amended accordingly. This has not happened.

The volume, nature and sensitivity of information—including personal information—contained under the broad umbrella of research and teaching materials is substantial. This would include everything from medical and health care trials, to social and cultural practices, to technical and scientific discoveries. There is no cogent reason why this information should not have the benefit of protection under Part 3 of FIPPA. [9]

Previous recommendations

The 1999 Special Committee recommended that FIPPA be amended to apply its privacy provisions to the teaching materials and research information of employees of post-secondary educational bodies, while maintaining their exemption from the access provisions of the Act. Our office restated this position in our 2015 submission, recommending that "FIPPA be amended to limit the exemption in s. 3(1)(e) to Part 2 of FIPPA."

Conclusion

Exempting teaching and research materials from FIPPA's access provisions in Part 2 of the Act only is a simple and complete answer to concerns regarding academic freedom and intellectual property. This amendment will preserve research and teaching materials from an access request while obligating those who possess such records to properly protect the personal information within them.

Recommendation 8
Amend FIPPA to limit the exemption in s. 3(3)(i) to Part 2 of FIPPA by moving it under s. 3(5).

[9] Indeed, this has been done in the new s. 3(5) of FIPPA, which limits other exemptions to only Part 2. Simply moving s. 3(3)(i) to be under s. 3(5) would address this longstanding concern.

Regulation to address privacy, transparency, and oversight for data-linking

Issue

Data-linking offers new opportunities for public body research and analysis, but carries with it a number of privacy challenges and risks. FIPPA does not offer any additional protections or oversight for this practice.

Discussion

Data-linking involves linking together or matching data about an identifiable individual in two or more data sets. This process can be used to create larger and more varied data for research and analysis.

Provisions around data-linking were added to FIPPA in 2011, along with new authorities that enabled public bodies to engage in greater information sharing. In particular, the authorities allow for the collection and disclosure of personal information for the broad purpose of "planning or evaluating a program or activity of a public body."

While data-linking can lead to new insights, it often involves using the personal information of citizens without their knowledge and consent.

The risks associated with data-linking are numerous, including its potential to produce inaccurate or misleading data, security concerns and vulnerabilities associated with broad sharing of large data sets, and the potential for surveillance and profiling.

To help address these risks, additional protections were added to FIPPA in 2011 that required public bodies to complete privacy impact assessments for data-linking initiatives, and to submit them to this office for review and comment. These obligations were triggered when the definition of 'data-linking' was met. However, the definition was widely acknowledged to be flawed, and this resulted in few, if any, such projects meeting the threshold for additional protection and oversight.

Recent amendments to FIPPA addressed the flawed definition of data-linking and require that all new initiatives, including data-linking, undergo privacy impact assessments.

While the recent amendments removed the requirement that a public body submit a PIA to my office for an initiative that involved data-linking, FIPPA provides for the creation of data-linking regulations after consultation with my office.

To date, government has undertaken data-linking initiatives, but as yet no regulatory rules have been put in place to guide them.

Other jurisdictions in Canada and elsewhere have developed comprehensive rules and standards for data-linking. For example, in 2018 Saskatchewan passed stand-alone legislation, the *Data Matching Agreements Act*, to govern this kind of activity in that province. More recently, Ontario enacted a comprehensive set of data standards for integrating data across ministries and other publicly-funded organizations.

The standards and rules elsewhere are varied, but generally focus on:

- bringing transparency to these initiatives through public notice or reporting;
- creating protections through technical safeguards, such as rules on encryption, de-identification, limiting the retention of personal information in order to not to store duplicate copies of databases or to create new large repositories of personal information from linked data;
- administrative requirements, such as the need for formal agreements between public bodies when engaging in joint data-linking initiatives;
- requirements to ensure that the personal information used and created about citizens is accurate; and
- the provision of oversight by requiring certain documentation to be sent to or made available to the regulator.

Conclusion

As noted, to date no regulatory rules have been put in place that would guide data-linking initiatives. These regulations should be drafted without delay, wherein a public body or bodies engaging in a data-linking initiative are required to adhere to an additional set of standards that bring transparency and additional privacy protections to their work.

As the government's presentation to the Special Committee in February conceded, there continues to be a need to provide for oversight over data-linking, and to ensure that the purpose of any such linking is appropriate and the personal information used is proportionate to achieve that purpose.

Previous recommendations

Both my office and the Special Committee recommended during the 2016 process that the definition of data-linking be amended to include linking together two or more data sets where the purpose of the linking differs from the original purposes of any of the linked data sets. The was meant to enable the oversight intended in the 2011 amendments.

The recommendations at the time also considered requirements and implications for data linking in the health care sector.

Recommendation 9
Government should draft and consult with the OIPC on regulations that address transparency, privacy protections and oversight for data-linking.

Privacy protection and regulation of the use of automated decision-making

Issue

Rapid advancements in automated decision-making systems, including those that employ artificial intelligence and data driven tools, can improve services by analyzing large amounts of data to find patterns, look for insights, and make recommendations. At the same time, the risks to privacy and other fundamental rights are such that enhanced protections are necessary.[10]

Discussion

Automated decision-making systems pose new risks to individual privacy by creating new information about individuals without their knowledge or consent, and without an assurance that the new information is accurate. These systems can also be used to make decisions about individuals, such as entitlements to public programs or the likelihood that they will engage in certain behaviours.

This technology is distinct from other technological advancements that largely increase efficiency—such as the difference between an online application system and a paper-based system—because it changes how a decision is made. It does not simply process applications *faster* than a more analog decision-making system, rather it processes applications *differently* and in a way that is not always clear to those running the system or the individual affected by the decision. Because of this phenomenon, specific measures are necessary to ensure the responsible and fair use of these systems by public bodies.

Regulatory landscape

Calls for the regulation of artificial intelligence have been increasing worldwide. The European Union recently published comprehensive draft regulations on the use of artificial intelligence that categorizes AI uses into risk categories, including some uses that are banned in all but the most limited circumstances.[11] This regulation is much more comprehensive than anything that exists in FIPPA, but is an example of where regulation is headed.

[10] Our office has jointly published an extensive report on the fairness and privacy concerns of Artificial Intelligence in the public sector. See *Getting Ahead of the Curve: Meeting the Challenges to Privacy and Fairness Arising from the Use of Artificial Intelligence in the Public Sector.*

[11] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM(2021) 206 final (Apr. 21, 2021) < https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206>.

Closer to home, both the federal Office of the Privacy Commissioner of Canada (OPC)[12] and the Newfoundland and Labrador Access to Information and Protection of Privacy Act, 2020 Statutory Review Committee[13] made similar recommendations on the subject of automated decision-making for their respective legislation.

The recommendations by the OPC were:

- The law should define automated decision-making.
- The law should include a right to meaningful explanation and human intervention related to the use of automated decision-making, as currently supported by the Treasury Board Secretariat's *Directive on Automated Decision-Making*.
- A specific standard should be denoted for the level of explanation required, so as to allow individuals to understand: (i) the nature of the decision to which they are being subject and the relevant personal information relied upon, and (ii) the rules that define the processing and the decision's principal characteristics.
- Where trade secrets or security classification prevent such an explanation from being provided, the following should at least be provided: (i) the type of personal information collected or used, (ii) why the information is relevant, and (iii) its likely impact on the individual.
- The law should contain an obligation for institutions to log and trace personal information used in automated decision-making.

The Newfoundland and Labrador recommendations were similar, but more focused on oversight than on creating new rights and obligations:

- Define "automated decision system".
- Define "algorithmic impact assessments" and require that any public body planning to implement an automated decision system complete one and, if requested, provide it to the commissioner.
- Require that public bodies notify the commissioner when developing a program or service using automated decision systems.
- Require public bodies to keep records of the decision-making processes of automated decision systems.
- Include monitoring and commenting on automated decision systems in the general powers and duties of the commissioner.

---

[12] OPC Submission to the Minister of Justice and Attorney General of Canada on the modernization of the *Privacy Act* (the Federal equivalent to Part 3 of FIPPA) < https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_jus_pa_2103/#fn44-rf>.

[13] Newfoundland, ATIPPA Statutory Review Committee, *Access to Information and Protection of Privacy Act, 2015: Statutory Review 2020* (June 2021) < https://www.gov.nl.ca/atipp/files/2020-Statutory-Review-ATIPPA-Final-Report.pdf>.

Also relevant to the Special Committee's considerations are how the matter of AI is being addressed in the private sector. The federal draft private sector bill[14], Quebec's Bill 64[15], and our submissions to the Special Committee to Review the Personal Information Protection Act all address the use of automated decision systems. As described in our supplementary submission to the PIPA Special Committee,[16] my office supports a model similar to Quebec's law that requires an organization using automated processing of personal information to:

- notify an individual that automated processing will be used to make a decision about them;
- on request, disclose the reasons and criteria used; and
- receive objections from individuals to the use of automated processing by someone within the organization who has the authority to review and change the decision.

Public bodies should be under no less of an obligation in respect to the use of these technologies, particularly as citizens do not have a choice about who processes their data (as opposed to the private sector, where options are available in terms of organizations that can provide services).

Current framework of FIPPA

Concerns about automated processing have long been recognized in FIPPA. Section 42(1)(g), which grants the Commissioner the power to comment on the implications for access to information or for protection of privacy of automated systems for collection, storage, analysis or transfer of information, has been in FIPPA since it first passed in 1992.

Public bodies also have the obligation under s. 31 of FIPPA to retain personal information "used by or on behalf of the public body to make a decision that directly affects an individual […] for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information." Satisfying this requirement may be difficult if a public body is unable to determine what information was used to make the decision in question.

Conclusion

FIPPA must be amended to ensure public bodies safely leverage automated decision-making systems. Meaningful explanations and the right of human intervention are necessary safeguards to help ensure the responsible introduction of this promising technology.

Previous recommendations

No recommendations on this subject have been made to previous Special Committees.

[14] Introduced in 2020 but not passed.
[15] Received assent on September 22 2021 and comes into force September 22, 2023.
[16] Supplemental submissions to the PIPA SC https://www.oipc.bc.ca/legislative-submissions/3513.

Recommendation 10
Define "automated decision-making."

Recommendation 11
Amend FIPPA to give individuals the right to be notified that automated decision-making will be used to make a decision about them, and, on request, receive a meaningful explanation of the reasons and criteria used. Individuals should also be given the right to submit an objection to the use of automated processing to an individual with the authority to review and change the decision. Require public bodies to create a record of how a decision is made that impacts an individual using automated decision-making in a format that is traceable. Where trade secrets or security classification prevent an explanation from being provided, the following should at least be provided: • the type of personal information collected or used; • why the information is relevant; and • its likely impact on the individual.

Comprehensive health information privacy legislation

Issue

British Columbia is the only province in Canada without a stand-alone health information law. Individuals, health care professionals, and researchers must instead navigate a patchwork of laws that apply to personal health information. This creates inefficiencies and uncertainty in all parts of the health care system.

Discussion

A number of laws and regulations cover personal health information in BC. A list of these is provided in Appendix A of this submission.

Most doctors' offices in the province operate under the private sector PIPA. In contrast, the Ministry of Health, health authorities, and most hospitals are subject to FIPPA. This means there are different privacy and information sharing rules in place depending on where a patient is being treated. As a result, personal health information disclosed under one law can be collected and used under another over the course of the same treatment.

Ten years ago, our office convened roundtable discussions on health research in an attempt to build consensus on appropriate privacy and security frameworks for the disclosure of personal information for health research. That work helped contribute to our 2014 report, *A Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector*.[17] The report noted that the legal frameworks in place at the time, which remain in place today, had not kept pace with the digital transformation of the health care sector. One of its primary recommendations was the need for clear and consistent rules for the public and the private sector.

While we continue to provide oversight over the use of personal health information under various laws and work directly with stakeholders in the interpretation and application of those laws, a more consolidated approach is long overdue.

Conclusion

Health information is among the most sensitive types of information and where our need for privacy is often most keenly felt. However, our information needs to be used, and sometimes shared, in order to deliver the health care services we rely on.

Both of these objectives can be better facilitated through a new and comprehensive health information privacy law.

Previous recommendations

We recommended the creation of a health information law to the 2014 Special Committee that reviewed PIPA, and to the FIPPA Special Committee the following year.

In both cases, the Committees agreed and made the same recommendation in their reports to the Legislative Assembly.

Recommendation 12
Government should enact new comprehensive health information privacy legislation.

[17] https://www.oipc.bc.ca/special-reports/1634

ENHANCED OVERSIGHT

Access to information and protection of privacy are becoming more and more consequential. These issues affect our democracy, our public services, our personal dignity and autonomy.

To ensure that access and privacy rules are adhered to, and that citizens have a meaningful avenue of redress, regulators are getting new tools and enforcement powers. At the federal level, the Access to Information Commissioner has been granted the order-making powers long sought by that office. At the same time, fines being levied by European regulators for the misuse of personal data are making headlines around the world.

Some progress has been made on strengthening the enforcement part of our law in BC. Bill 22 added offences provisions for snooping and for evading access requests. But more needs to be done to ensure that our office has the ability to uphold access rights and to protect privacy, as well as to ensure that our operations are as efficient as possible in our service to British Columbians.

Consultation on draft legislation that affects access and privacy

Issue

The Commissioner has the power to comment on the implications for access to information or for the protection of privacy of proposed legislative schemes, but there is no requirement for government to consult with this office on draft legislation.

Discussion

There are policies and procedures for ministries to provide draft legislation to this office, when those initiatives may have access or privacy implications. As Commissioner, I have signed undertakings and confidentiality agreements to support this process.

Despite these efforts to ensure that the Commissioner can exercise their statutory functions, and that ministries can benefit from the review process, there have been times when this arrangement has not worked effectively.

In other jurisdictions, the requirement to consult with the Commissioner or supervisory authority on proposed legislation is explicitly set out in the law. This alleviates any uncertainty in terms of whether such consultations can or need to occur.

For example, Europe's General Data Protection Regulation (GDPR) states that, "Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament or of a regulatory measure based on such a legislative measure, which relates to processing [of personal data]" (Article 36(4)).

In Canada, a similar requirement is found in Newfoundland and Labrador's *Access to Information and Protection of Privacy Act*. That Act contains the following section, which could easily be adapted for our own legislation:

> **Amendments to statutes and regulations**
>
> **112.** (1) A minister shall consult with the commissioner on a proposed Bill that could have implications for access to information or protection of privacy, as soon as possible before, and not later than, the date on which notice to introduce the Bill in the House of Assembly is given.
>
> (2) The commissioner shall advise the minister as to whether the proposed Bill has implications for access to information or protection of privacy.
>
> (3) The commissioner may comment publicly on a draft Bill any time after that draft Bill has been made public.

Previous recommendations

The 1999 Special Committee considered this issue in its report to the Legislative Assembly, saying that the Commissioner's independence and integrity could be undermined should they provide advice to government on the effects of draft legislation or regulations on access and privacy.

Our office made this recommendation to the next Special Committee in our 2004 submission. In response, that Committee encouraged public bodies to informally ask for the Commissioner's comments on draft bills before their introduction.

Conclusion

Consultation with this office on draft legislation that may have access or privacy implications allows ministries to benefit from the Commissioner's expertise, and if necessary, to amend a bill to reflect discussions with the OIPC before it is introduced.

These consultations are confidential, and in no way waive the government's solicitor client or Cabinet privilege.

Recommendation 13
Require ministries to consult with the OIPC on draft legislation that could have implications for access to information or protection of privacy.

Harmonization of section 56 of FIPPA with PIPA

Issue

Section 56(6) of FIPPA requires that an inquiry into a matter under review must be completed within 90 days after receiving the request for review. However, the majority of these files take longer to resolve and FIPPA is silent about the Commissioner's ability to extend the review period.

Discussion

An applicant can ask my office to review the decision of a public body if access to all or part of a record is refused. Once this request is made, my office has 90 days to complete an inquiry into the matter.

We seek to provide all applicants with fair and timely access to our services; however, this is challenging as the volume of requests for review continues to be high and my office has limited resources.

The review period often needs to be extended to ensure the OIPC continues to have jurisdiction in the event the matter proceeds to an inquiry. While the vast majority of requests for review are successfully settled without the need for an inquiry, this process takes time. In the last fiscal year, 59% of review files required more than the 90 days to resolve.

Traditionally, we have dealt with this issue by seeking the consent of each party to hold an inquiry outside the 90-day period. While this approach has been successful, it is confusing for applicants who believe declining to consent will result in an inquiry being conducted sooner when the reality is that OIPC will lose jurisdiction if consent is declined.

Extending the review period is not an issue in Alberta's *Freedom of Information and Protection of Privacy Act*,[18] or in BC's private sector privacy law. In both cases, the tribunal can extend the review period so long as notice is provided to the parties along with the anticipated or later date for completing the review.

A similar provision in FIPPA would give certainty to the process required to extend the review period. Adding this to the legislation would reduce confusion, and if used effectively, can give a better sense to applicants of when they can expect the review to be complete.

The preference is to bring consistency between s. 56(6) of FIPPA and the process set out in s. 50(8) of PIPA, which reads as follows:

[18] Section 69(6).

> 50(8) An inquiry respecting a review must be completed within 90 days of the day on which the request is delivered under section 47(1), unless the commissioner
>
> (a) specifies a later date, and
>
> (b) notifies
>
> (i) the individual who made the request,
>
> (ii) the organization concerned, and
>
> (iii) any person given a copy of the request of the date specified under paragraph (a).

Previous recommendations

This office has made this recommendation to every Special Committee since 2004. It was not supported when it was first put forward, but has been supported and recommended by the last two Special Committees.

Conclusion

The limited review period in FIPPA for requests for review can help to encourage a timely settlement. However, most files take longer to resolve, and uncertainty with regards to extensions slows down this process. A clear and straight-forward approach is more efficient and consistent with PIPA and with other public sector privacy laws.

Recommendation 14
Amend s. 56 of FIPPA to permit the Commissioner to extend the 90-day review period in a manner that is consistent with s. 50(8) of PIPA.

Facilitating regulatory collaboration

Issue

FIPPA does not explicitly address the Commissioner's ability to share information with regulatory counterparts outside of a formal investigation. This can a pose barrier to the Commissioner's ability to meaningfully consult with regulators in similar roles on emerging issues that have cross jurisdictional implications.

Discussion

The Office of the Information and Privacy Commissioner for BC works with access and privacy regulators across Canada and around the world, as well as with other Independent Officers of the Legislature here in BC. The need for this collaboration is increasing as emerging issues cross jurisdictional boundaries, both in terms of geography and regulatory spheres. A good example of this is our recent report on the challenges to privacy and fairness arising from the use of

artificial intelligence in the public sector, which we undertook in collaboration with the BC Ombudsperson and the Yukon Ombudsperson and Information and Privacy Commissioner.

FIPPA restricts the Commissioner's ability to share information obtained in the performance of their duties and functions. While these restrictions are important as the Commissioner often handles confidential information, they can impair this important collaboration with regulatory counterparts outside of a formal investigation.

This means that when dealing with an emerging privacy issue, such as the use of contact tracing for COVID-19, the Commissioner may be unable to share information about the work of public bodies in British Columbia with other provincial or federal regulators who may be dealing with the same or similar concerns. This sharing can assist the work of our office in determining further actions.

PIPA recognizes the need for collaboration with other regulators, as it specifically authorizes, "the exchange of information with any person who, under legislation of another province or of Canada, has powers and duties similar to those of the commissioner." This kind of provision should be imported into FIPPA as well. Doing so can facilitate enforcement collaboration, including through the sharing of knowledge and best practices, and enable regulators to maximize the use of resources.

A similar proposal was recently made in the Government of Canada's White Paper on reform to the federal public sector *Privacy Act*.[19] In that paper, the federal government noted that an information sharing provision found in their private sector legislation (the *Personal Information Protection and Electronic Documents Act*) could serve as a model for a similar section in the public sector law. This proposal to allow for greater information sharing with relevant oversight bodies and other regulators has the support of the federal Office of the Privacy Commissioner.[20]

Conclusion

Issues around access and privacy have become far more complex in the digital environment. This can spur a greater need to collaborate and learn from other regulators, both within and outside the province. While this can occur in the context of a formal investigation, there are other contexts when sharing information can enhance and further collaboration. This information sharing should be subject to legal parameters, as is the case in PIPA.

[19] RSC 1985, c P-21.
[20] Canada, Office of the Privacy Commissioner, *Submission on Bill C-11, the Digital Charter Implementation Act* (Ottawa: May 2021) <https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/>.

Recommendation 15
Amend FIPPA to allow the Commissioner to share information with regulatory counterparts to facilitate enforcement collaboration.

Disclosures by the Commissioner in the public interest

Issue

FIPPA does not give the Commissioner any discretion to disclose information collected in the course of their work where it is in the public interest to do so. The Commissioner's ability to disclose information is limited to situations where it is necessary to conduct an investigation, audit or inquiry, or to establish the grounds for findings or recommendations made in a report under the Act.[21] This is in contrast to many other jurisdictions at home and around the world where Commissioners can disclose information where it is in the public interest to do so.

Discussion

While the prescribed areas for the disclosure of information noted above have a clear and definite purpose, having *no* ability to disclose information beyond those areas limits our office's effectiveness to serve the broader public interest.

The majority of our work with public bodies is and should remain confidential, but there are critical occasions where the public interest would be properly served by our office's ability to disclose information outside of a formal order or report.

For example, where our office discovers an issue with a public body's security system in the course of our work, being able to disclose that issue to other public bodies would allow those other public bodies to mitigate risks they would not otherwise necessarily known about. In other words, the public interest in having the information more broadly disclosed would outweigh FIPPA's general rule of confidentiality.

Provisions that allow for greater discretion in the disclosure of information have been present in other jurisdictions for decades. For example, New Zealand's legislation states that:

> the Commissioner may disclose any matters that in the Commissioner's opinion ought to be disclosed for the purposes of giving effect to this Act.[22]

[21] Section 47. Under this provision the Commissioner may also disclose information obtained in the performance of their duties to give evidence in certain proceedings or to the Attorney General (s. 47).
[22] Privacy Act 2020 (NZ), section 206.This authority is subject to a few conditions, such as restrictions around the disclosures that may impact security or international relations, cabinet confidences, etc. The same wording has been present in New Zealand since the first iteration of the Privacy Act 1993.

In the United Kingdom, the Commissioner may disclose confidential information if:

> having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest.[23]

In Canada, the federal Privacy Commissioner has a similar authority in the *Personal Information Protection and Electronic Documents Act,* which states that:

> The Commissioner may, if the Commissioner considers that it is in the public interest to do so, make public any information that comes to his or her knowledge in the performance or exercise of any of his or her duties or powers under this Part [Protection of Personal Information in the Private Sector].[24]

In Australia, a proposal to allow the Commissioner to disclose information acquired in the course of their privacy functions is also under consideration. In a similar fashion, that proposal would grant the Commissioner the ability to disclose information about a number of investigative actions and outcomes, or when satisfied that it is in the public interest to make a disclosure.[25]

FIPPA has an existing provision that requires all public bodies, including my office, to disclose, without delay, information in the public interest.[26] This is a mandatory requirement that overrides all other parts of the Act, and should only apply in the most limited and compelling circumstances. The disclosure authority contemplated here would instead be discretionary and specific to the work of the Commissioner.

Conclusion

Many of the materials that come before my office are given in confidence and deal with sensitive matters. It is entirely appropriate and necessary for FIPPA to limit the disclosure of that information. This should give comfort and assurance to public bodies that are subject to an action by the Commissioner or who seek to consult with the Commissioner on a proposed initiative or other matter. However, the current restriction in s. 47 is overly broad and can delay or prevent the disclosure of information when doing so is the public interest.

---

[23]Data Protection Act 2018 (UK)section 132(2)(f). The identical wording was found in the Data Protection Act 1998 (UK), section 59(2)(e). A similar power of discretionary disclosure was also provided to the precursor of the UK Information Commissioner, the Data Protection Registrar in the Data Protection Act 1984 (UK), section 36(3).

[24] Section 20(2).

[25] Pg 22: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf and at pg. 48 https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-exposure-draft.pdf

[26] S. 25.

Recommendation 16
Amend s. 47 of FIPPA to allow the Commissioner to disclose information obtained in the course of their duties when the disclosure is in the public interest.

Consolidation and review of other statutes that prevail over FIPPA

Issue

More than 40 BC statutes have provisions that override or prevail over FIPPA in whole or in part. While these provisions may have merit, their overall effect is to weaken the breadth and coverage of FIPPA. A mechanism is needed to periodically review these provisions so that those that are no longer needed or that go beyond what is necessary can be amended or repealed.

Discussion

Section 3(7) of FIPPA states that where there is a conflict between FIPPA and any other provincial statute, FIPPA prevails unless the other statute expressly states that it overrides FIPPA. This provision demonstrates that the Legislature intended the access to information and protection of privacy provisions in FIPPA to take precedence over other statutes, except in extraordinary or unique circumstances.

At times, the overrides are meant to ensure the confidentiality that FIPPA already provides. In other words, the objective of the override can already be met by the exceptions to disclosure in FIPPA, which require or allow public bodies to withhold information. What an override often does is ensure that there is no chance that certain records will be disclosed, either through error or a public body not exercising its discretion to withhold information.

This is not to say that there should not be any overrides of FIPPA. Section 3(7) acknowledges that some overrides will occur, and in some cases, this office has supported these extraordinary measures. However, the number of overrides is significant and there is no mechanism to review them.

In Newfoundland and Labrador there is a process for this written into their legislation. A schedule in their *Freedom of Information and Protection of Privacy Act* lists provisions in other statues that prevail over that Act.[27] And there is a requirement that the Special Committee that reviews FIPPA in that jurisdiction consider the list of override provisions to determine if they are still needed.[28] This process has recently taken place, and resulted in recommendations to add an override to the Act and to remove several others.[29]

[27] Schedule A
[28] Section 117(2)
[29] https://www.nlatippareview.ca/files/FINAL-REPORT-June-8-2021-2.pdf

Previous recommendations

The recommendation to list provisions in statutes that prevail over FIPPA in a schedule to the Act, and to amend s. 80 to include a review of those provisions as part of the statutory review, was made by our office to the last Special Committee.

The Special Committee agreed that this was an issue and recommended the appointment of a committee to review of the existing overrides of FIPPA and make recommendations as to whether they should be amended or repealed.

Conclusion

Overrides of our right of access should only occur in the most exceptional circumstances, especially given that FIPPA already strikes a balance between making records available and the need for confidentiality. Despite this, there are already a large number of overrides and they continue to be added. A periodic review of these overrides can help to ensure that they are still needed and protect the integrity of FIPPA.

Furthermore, the listing of the overrides in the FIPPA gives them greater transparency, which helps to understand their overall breadth and impact, and makes it easier for those required to adhere to them to see when they apply.

Recommendation 17
Amend Part 6 of FIPPA to require government to list provisions in statutes that prevail over FIPPA in a schedule to the Act, and amend s. 80 of FIPPA to include a review of those provisions as part of the statutory review of the Act.

CONCLUSION

The recommendations made in this submission focus on strengthening transparency and accountability in the public sector and on offering further protections to citizen's privacy as public bodies seek to collaborate and leverage new technologies that make use of our personal information.

Public sector transparency and privacy are integral to good government and individual rights and autonomy. The recommendations that the Special Committee makes in advancing the existing aims and purposes of FIPPA will be of critical importance. I would truly hope that the efforts of the Special Committee members not end with the filing of their report to the Legislative Assembly. I would strongly urge you to continue your efforts to advocate your findings and conclusions to the government to ensure your considerable efforts involved with your review bear legislative fruit.

SUMMARY OF RECOMMENDATIONS

Recommendation 1: Include the administrative functions of the Legislative Assembly as a public body under FIPPA in such a way that maintains the important role that constituency records and other records subject to parliamentary privilege play in our democratic process.

Recommendation 2: Amend FIPPA to allow the Executive Council to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees when they are satisfied that the public interest in the disclosure outweighs the need to protect cabinet confidences.

Recommendation 3: Amend s. 13(1) of FIPPA to clarify the following:

- "advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process, and to that extent, are similar concepts and often interchangeably used terms;
- "advice" or "recommendations" does not apply to the facts upon which the advice or recommendation is based; and
- "advice" or "recommendations" does not apply to factual, investigative, or background material, for the assessment or analysis of such material, or for professional or technical opinions.

Recommendation 4: Clarify the language in s. 2 to specifically state that despite any common law or legal exemption to disclosure, public bodies may only rely on the specific exceptions contained in FIPPA.

Recommendation 5: Add to s. 29 of FIPPA a requirement that public bodies correct personal information when an individual requests that their personal information be corrected - if the public body is satisfied on reasonable grounds that the request made should be implemented.

Recommendation 6: Amend FIPPA to require that public bodies have in place reasonable measures respecting records management.

Recommendation 7: Amend s. 42 of FIPPA to expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records. The Commissioner should have jurisdiction over the unauthorized destruction of records as set out in:

- any enactment of British Columbia, or
- set out in a bylaw, resolution or other legal instrument by which a local public body acts or, if a local public body does not have a bylaw, resolution or other legal instrument setting out rules related to the destruction of records, as authorized by the governing body of a local public body.

Introduce offenses and penalties tied the above obligations.

Recommendation 8: Amend FIPPA to limit the exemption in s. 3(3)(i) to Part 2 of FIPPA by moving it under s. 3(5).

Recommendation 9: Government should draft and consult with the OIPC on regulations that address transparency, privacy protections and oversight for data-linking.

Recommendation 10: Define "automated decision-making."

Recommendation 11: Amend FIPPA to give individuals the right to be notified that automated decision-making will be used to make a decision about them, and, on request, receive a meaningful explanation of the reasons and criteria used. Individuals should also be given the right to submit an objection to the use of automated processing to an individual with the authority to review and change the decision.

Require public bodies to create a record of how a decision is made that impacts an individual using automated-decision making in a format that is traceable.

Where trade secrets or security classification prevent an explanation from being provided, the following should at least be provided:

- the type of personal information collected or used;
- why the information is relevant; and
- its likely impact on the individual.

Recommendation 12: Government should enact new comprehensive health information privacy legislation.

Recommendation 13: Require ministries to consult with the OIPC on draft legislation that could have implications for access to information or protection of privacy.

Recommendation 14: Amend s. 56 of FIPPA to permit the Commissioner to extend the 90-day review period in a manner that is consistent with s. 50(8) of PIPA.

Recommendation 15: Amend FIPPA to allow the Commissioner to share information with regulatory counterparts to facilitate enforcement collaboration.

Recommendation 16: Amend s. 47 of FIPPA to allow the Commissioner to disclose information obtained in the course of their duties when the disclosure is in the public interest.

Recommendation 17: Amend Part 6 of FIPPA to require government to list provisions in statutes that prevail over FIPPA in a schedule to the Act, and amend s. 80 of FIPPA to include a review of those provisions as part of the statutory review of the Act.

APPENDIX A: PIECES OF LEGISLATION AFFECTING PERSONAL HEALTH INFORMATION IN BC

Continuing Care Act
Authorizes the Ministry and a health authority to require a person to provide information respecting the person or the members of the person's family thought necessary for the proper administration of the Act.

E-Health (Personal Health Information Access and Protection of Privacy) Act
Governs the collection, use and disclosure of personal health information through electronic databases of the Ministry and health authorities that have been designated by the Minister as "health information banks".

Freedom of Information and Protection of Privacy Act
Applies to personal information that is in the custody or control of the Ministry, health authorities, agencies, boards and commissions in the health sector (including the Medical Services Commission) and professional regulatory bodies.

Health Authorities Act
Requires a regional health board to disclose personal information in a report made to the Minister.

Health Professions Act
Addresses the collection of personal information by regulatory colleges and provides rules with respect to the disclosure of personal health information by pharmacists.

Hospital Insurance Act
Authorizes the Ministry or a hospital to require a person to provide information respecting the person or the members of the person's family thought necessary for the proper administration of the Act.

Laboratory Services Act
Governs the collection, use and disclosure of personal information by the Ministry in relation to the payment of benefits for laboratory services.

Medical Research (BC Cancer Agency) and Health Status Registry Act
In conjunction with the British Columbia Cancer Agency Research Information Regulation, authorizes the collection and disclosure of personal information to facilitate medical research into the prevention, causes, diagnosis, treatment and outcomes of cancer.

Medicare Protection Act
Provides that individuals must keep matters about beneficiaries and practitioners that come to

their knowledge in the course of administering the Act confidential subject to certain exceptions.

Ministry of Health Act
Authorizes the collection, use and disclosure of personal information by the Ministry from a public body for a stewardship purpose.

Personal Information Protection Act
Applies to personal information that is in the custody or control of organizations, including private practices of health professionals and private labs.

Pharmaceutical Services Act
Provides for the collection of personal information to provide health services, or facilitate care, in relation to drugs, devices, substances and related services; and for the use and disclosure of personal information for a number of prescribed purposes.

Public Health Act
Provides authority for the collection, use and disclosure of personal information related to reporting disease, health hazards and other matters.

APPENDIX B: BC STATUTES WITH PROVISIONS THAT PREVAIL OVER FIPPA

Legislation	**Sections with clauses that fully or partly prevail over FIPPA**
Administrative Tribunals Act	61
Adoption Act	70(3), 74
Adult Guardianship Act	46(1)
Animal Health Act	16(2), 60(a)
Architects Act	51.2(3)
Child, Family and Community Service Act	24(2), 74, 75, 77, 96
Civil Resolution Tribunal Act	90(1)
Coroners Act	64, 66
Criminal Records Review Act	6(4)
E-Health (Personal Health Information Access and Protection of Privacy) Act	20(1)
Election Act	275(7)
Emergency Communications Corporations Act	9(3), 9(4)
Employer Health Tax Act	90(9)
Employment Standards Act	75(2), 101(2)
Evidence Act	51(7)
Family Law Act	11(2), 133(4), 243(3)
Family Maintenance Enforcement Act	43(1)
Health Professions Act	26.2(6)
Heritage Conservation Act	3(3)
Income Tax Act	64(8)
Laboratory Services Act	29(1)
Legal Profession Act	88(2), (7) & (8)
Local Elections Campaign Financing Act	63(3)
Local Government Act	49
Mines Act	34(8)
Missing Persons Act	21(1)
Motor Vehicle Act	93.1
Pharmaceutical Services Act	7, 25
Pharmacy Operations and Drug Scheduling Act	16(1)(c)
Police Act	182
Professional Governance Act	110(7)
Provincial Immigration Programs Act	10(2)
Public Guardian and Trustee Act	17(3)
Public Health Act	53
Public Inquiry Act	26(1), 28(7)

Public Interest Disclosure Act	51(2)
Recall and Initiative Act	168(8)
Securities Act	148(2)
Speculation and Vacancy Tax Act	120(10)
Statistics Act	9(2)
Teachers Act	53(9)
Temporary Foreign Worker Protection Act	34(2)
Vancouver Charter	8.1
Victims of Crime Act	7(2)
Witness Security Act	38(2)