OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Submission of the A/Information and Privacy Commissioner to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*

March 15, 2010

TABLE OF CONTENTS

SUMMARY OF RECOMMENDATIONS

SUBMISSIONS ON PRIVACY PROTECTION

1. Amend s. 2 of FIPPA to require that for an infringement of the right to privacy to be lawful, it must be proportional to the public interest that is achieved.

2. Government should not proceed with any more data sharing initiatives until a meaningful public consultation process has occurred, and the outcome of that process is an enforceable code of practice for data sharing programs.

3. A Government Chief Privacy Officer should be appointed.

4. FIPPA should be amended to give the OIPC a statutory mandate to review and approve all data sharing initiatives.

5. Amend FIPPA to require that data sharing projects for the purpose of research must be subject to ethics review by an arm's length stewardship committee.

6. Add a requirement in FIPPA that privacy impact assessments must be completed at the conceptual, design, and implementation phases of an electronic record project. This requirement should apply to health authorities as well as to ministries of government.

SUBMISSIONS ON IMPROVING ACCESS IN THE 21ST CENTURY

7. Add a new section at the beginning of Part 2 of the Act requiring public bodies to adopt schemes approved by the Commissioner for the routine disclosure of electronic records, and to have them operational within a reasonable period of time.

8. Amend s. 9(2) of FIPPA to require that public bodies release electronic records in electronic form where the record can reasonably be reproduced in electronic form.

9. (a) Amend FIPPA to give the Commissioner the power to investigate and ensure compliance with the *Document Disposal Act* or compliance with rules relating to the destruction of records.

   (b) Add to FIPPA a "duty to document" key prescribed government decisions.

10. Amend s. 25 to require pro-active disclosure despite any other provision of FIPPA where there is a significant public interest in the disclosure that outweighs any potential harm from the disclosure.

11. (a) Amend FIPPA so that paragraph (n) of the definition of local government body is moved into the definition of public body in Schedule 1.

    (b) Amend s. 3 to clarify that records created by or in the custody of a service-provider under contract to a public body are under the control of the public body on whose behalf the contractor provides services.

12. Amend s. 71 of FIPPA to require that public bodies make available to an individual his or her own personal information free of charge and without an access request, but subject to any access exceptions under the Act.

13. Amend s. 3 of the 1993 FIPPA Regulation to make it consistent with ss. 1 to 4 of the PIPA Regulation.

14. Amend s. 4(1) to establish that an applicant who makes a formal access request has the right to anonymity throughout the entire process.

15. Amend s. 13(1) to clarify the following:

    (a) "advice" and "recommendations" are similar and often interchangeably used terms not sweeping separate concepts,

    (b) "advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process,

    (c) the "advice" or "recommendations" exception is not available for the facts upon which advice or recommended action is based,

    (d) the "advice" or "recommendations" exception is not available for factual, investigative or background material, for the assessment or analysis of such material, or for professional or technical opinions.

16. Repeal s. 20(1)(a) and amend s. 3(1) to state that the Act does not apply to records available for purchase by the public.

17. Amend s. 22(2) to state that the personal information of an individual who has been dead for over 20 years is a relevant consideration in determining whether the disclosure of the deceased's personal information would be an unreasonable invasion of personal privacy.

SUBMISSIONS ON IMPROVING OIPC PROCESSES

18. FIPPA should be amended 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.

19. FIPPA should be amended by adding a new section that would explicitly permit the Commissioner to review records that are being withheld by a public body on the basis of solicitor-client privilege in order to verify that the privilege applies. The amendments should:

    1. Give the Commissioner specific, explicit authority to investigate, inquire into and issue orders concerning whether a public body or organization is authorized to refuse access to information or records on the ground of solicitor-client privilege under s. 14 of FIPPA; and

    2. Expressly preserve and protect the substantive solicitor-client privilege despite the Commissioner's confidential examination of records in issue, when examination is necessary to verify the existence of the privilege.

    3. The Commissioner's discretion to disclose information relating to the commission of an offence to the Attorney General pursuant to s. 47(4) of FIPPA should be removed.

20. Amend s. 42 to explicitly give the Commissioner the power to require public bodies to submit statistical and other information related to their processing of freedom of information requests, in a form and manner that the Commissioner considers appropriate.

21. Amend s. 59(2) and a new s. 59(3) should be added to inhibit abuse of the judicial review process by time-limiting the automatic stay of the Commissioner's order as follows:

    1. If an application for judicial review is brought before the end of the period referred to in subsection (1), the order of the Commissioner is stayed for 60 days from the date the application is brought.

    2. A court may abridge or extend, or impose conditions on, a stay of the order of the Commissioner under subsection (2).

22. Amend s. 56 of FIPPA to permit the Commissioner to extend the 90 day timeline to review requests in a manner that is consistent with s. 50(8) of PIPA.

A. INTRODUCTION

[1] For nearly two decades, the *Freedom of Information and Protection of Privacy Act* ("FIPPA") guaranteed the right to access information and the protection of privacy. It is a foundation upon which government remains open and accountable to the public. Our submissions are essentially aimed at keeping the Act current. As public expectations, government practices, legal interpretations and information technology evolve, so must the legislation to ensure its purposes are achieved and its continued relevance in a changing world.

[2] Just as freedom of information law is a fundamental aspect of any democratic government, balanced and enforceable privacy rights are necessary to protect citizens from the power of the state. While access to information and protection of privacy rights are complementary they serve distinct purposes.

[3] Freedom of information is about making public institutions accountable to the citizens they serve. While still the leader of the Official Opposition in July 1998, the current premier, Gordon Campbell stated:

> Open government is the hallmark of a free and democratic societ[y].
>
> Access to government information helps us, as the Official Opposition, and others hold the government to account, and accountability enhances democracy. When government does its business behind closed doors, people will invariably believe that government has something to hide. Secrecy feeds distrust and dishonesty. Openness builds trust and integrity.
>
> But FOI is not just a tool of Opposition. The fundamental principle must be this: government information belongs to the people, not to government. This means, among other things, that all citizens must have timely, effective and affordable access to the documents which governments make and keep. Government should facilitate access, not obstruct it.[1]

[4] Former federal Information Commissioner, Robert Marleau spoke of:

> .. the awesome responsibility to safeguard that essential building block of democratic freedom – the ability of citizens, as of right, to obtain access to government-held records. Throughout the world, the lesson of history is consistent: Openness is the oxygen of democracy because, to mix a metaphor, sunshine is the best disinfectant. Courageous parliamentarians and governments fought for and gave Canadians [freedom of information legislation]. The challenge is to make a good law better and help our excellent public officials become even more comfortable with ever increasing degrees of transparency.[2]

---

[1] July 22, 1998 letter from Gordon Campbell to Darrell Evans, BC Freedom of Information and Privacy Assn.

[2] Office of the Information Commissioner, Annual Report 2006-2007, *Chapter 1: Summing Up*.

[5] Chief Justice of Canada, Beverly McLachlin stated:

> The need for information is compounded by the inevitable tendency of governments, and those exercising powers on behalf of the government, to disclose only as much as they deem necessary. Despotic secrecy is the historic norm. Democracy sets its face against this. Yet, unchecked, the tendency is always there. And unchecked, it will inevitably undermine democracy.[3]

[6] Statesmen and scholars have recognized this. In the words of Pierre Elliott Trudeau:

> ... the democratic process requires the ready availability of true and complete information. In this way people can objectively evaluate the government's policies. To act otherwise is to give way to despotic secrecy.[4]

[7] Privacy protection is also a fundamental value in a modern, democratic society. Information privacy, like other kinds of privacy, is based on the concept of the dignity and integrity of the individual. Canadian courts have repeatedly recognized the importance of information privacy:

> In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained ... .[5]

[8] Governments are increasingly turning to sophisticated electronic information systems to collect, share, analyze, compile and store often extremely sensitive personal information of citizens. As governments rely more and more on electronic systems, privacy challenges will continue to grow.

[9] The Special Committee has a unique opportunity to recommend amendments that would ensure that government continues to be accountable to its citizens and the public's right of access to information under FIPPA remains meaningful. The Special Committee also has the opportunity to recommend

---

[3] Remarks of the Right Honourable Beverley McLachlin, P.C. Chief Justice of Canada: *Access to Information and Protection of Privacy in Canadian Democracy*, May 5, 2009.

[4] Pierre Elliott Trudeau, quoted by G. Baldwin, M.P. in Standing Joint Committee on Regulations and other Statutory Instruments, *Minutes of Proceedings and Evidence*, 30th Parl., 1st Sess. (1974-75), 22:7 as cited in T. Murray Rankin, *Freedom of Information in Canada: Will the Doors Stay Shut?* (Ottawa: Canadian Bar Association, 1979).

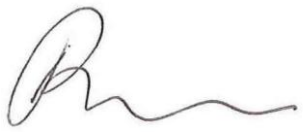
[5] See *R. v. Dyment*, [1988] 2 S.C.R. 417 at pp. 429-430.

amendments to ensure FIPPA's privacy protections remain strong and consistent with advances in information technology.

[10] Our submission is divided into three major areas: improving access, protecting privacy, and improving our processes. A common theme in the areas of access and privacy is the need to update FIPPA to take into account the use and potential of information technology. Where relevant, this submission includes previous recommendations that the Office of the Information and Privacy Commissioner ("OIPC") and the 2004 Special Committee made, as well as government's response to those recommendations. We have also presented comparative information with respect to our recommendations, particularly on legislation analogous to FIPPA in other Canadian jurisdictions and internationally.

Victoria, British Columbia

March 15, 2010



Paul D.K. Fraser, Q.C.
A/Information and Privacy Commissioner
for British Columbia

B. PRIVACY PROTECTION

PRIVACY INFRINGEMENTS MUST BE REASONABLE AND JUSTIFIABLE

[11] Canadians are concerned about privacy. This concern is fuelled by the increasing number of privacy breaches, the growth of and reliance on large networked electronic databases, the increase in government surveillance of citizens and government data matching schemes.

[12] FIPPA attempts to pro-actively examine the privacy risks inherent in any new project, program, system or legislation by requiring government ministries to conduct "privacy impact assessments" (PIA). In our view these PIA's, while important, are insufficient. They are insufficient because they are essentially compliance reviews, and fail to identify and justify the privacy risk any initiative creates for the personal privacy of individuals whose lives and personal information are affected. They fail to address the fundamental question of whether or not the privacy intrusion is "reasonable and justifiable."

[13] The concept that an infringement of the right to privacy must be reasonable and justifiable is found in s. 2 of the *Personal Information Protection Act* ("PIPA") which sets out the purposes of that Act as follows:

> The purpose of this Act is to govern the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[14] However, no such provision exists in FIPPA. In our submissions to the 2004 Special Committee we recommended FIPPA be amended to require public bodies to consider the wider privacy impacts created by a proposal, and if those impacts could not be minimized to an acceptable level, the proposal should be abandoned.

[15] This recommendation followed a 2001 proposal by Senator Sheila Finestone, P.C. to create a legislative "Privacy Rights Charter." Senator Finestone discussed the purpose of the Charter:[6]

> Let us also not forget that a hallmark of authoritarian societies … is a capacity to collect information about citizens, to monitor their behaviour, often without their knowledge or consent, and to use that surveillance to make them fearful of exercising the rights that attach to a democracy.

---

[6] Privacy Rights Charter (Bill S-21), Senate of Canada, 1st Session, 37th Parliament, http://www.parl.gc.ca/37/1/parlbus/chambus/senate/bills/public/pdf/s-21_1.pdf.

> At the heart of the Privacy Rights Charter, in its preamble, is the recognition of privacy as a basic human right and a fundamental value. It is a defining difference between an authoritarian state and one built on democratic principles.
>
> It reflects Canada's commitment as a signatory to international human rights instruments to honour and promote privacy. It acknowledges privacy as an interest in the public good, one that is essential to the preservation of democracy and the exercise of many of the rights and freedoms guaranteed by Canada's *Charter of Rights and Freedoms*.
>
> This Charter seeks to give effect to several principles:
>
> - first, that privacy is essential to an individual's dignity, integrity, autonomy and freedom, and to the full and meaningful exercise of human rights and freedoms;
> - second, that there is a legal right to privacy; and,
> - third, that an infringement of the right to privacy, to be lawful, must be reasonable and justifiable.

[16] We propose another means of achieving this goal—by amending the purpose statement in s. 2 of FIPPA to reflect the concept that any privacy infringement by government be "reasonable and justifiable." Like any other right, privacy rights may be secondary to other public interest objectives—where the infringement is reasonable and can be demonstrably justified in a free and democratic society. The extent of the infringement must be proportional to public interest that is achieved.

Recommendation #1:

Amend s. 2 of FIPPA to require that for an infringement of the right to privacy to be lawful, it must be proportional to the public interest that is achieved.

DATA SHARING PLANS CREATE SIGNIFICANT PRIVACY CONCERNS

[17] New information technologies enable data sharing initiatives on a scale and frequency that were never contemplated at the time FIPPA was drafted. The ever increasing size and numbers of electronic databases and the new and novel ways in which the personal information they contain is being collected, used and disclosed in data sharing projects raise significant privacy issues.

[18] "Data sharing" is the programmatic or planned disclosure of personal information by one government agency to another, by one government to another

government, or by a government to a private sector organization. It is a growing phenomenon because of the existence of electronic databases from which massive amounts of information can be disclosed, matched, or mined in the blink of an eye. They may be one-off disclosures or regular, planned exchanges or matches of data. Data sharing is likely to occur between or among networked or connected databases rather than depending on the creation of large mega databases. [The term "data sharing" as used here would include the related activities of data-matching or data-mining.]

[19] "Data-matching" is the large scale comparison of information that has been collected for different purposes, with a view to identifying commonalities or matters of interest.

[20] "Data mining" is the process of extracting patterns from data. Large volumes of data are analyzed using techniques, such as statistical analysis and modeling, to uncover hidden patterns or relationships. Data mining is commonly used in a wide range of profiling practices such as marketing, surveillance and fraud detection.

[21] The term "dataveillance" is used to describe the social sorting that results when data collected for disparate purposes is reconfigured to create a new digital profile of a citizen. An illustrative example was reported in the Ottawa Citizen last year. A man living on an aboriginal reserve was denied a loan because of his postal code. His postal code was included in a category of postal codes that the bank had deemed unsuitable. His personal credit history was apparently of no consequence. Using data about him—where he lived as determined by the geographic tag of his postal code—the bank slotted him into a socio-economic class and on that basis decided he didn't merit a loan.

[22] When there is a bulk disclosure of personal information from a large database of one public body to another public body, citizens usually do not know how their personal information is being reconfigured, who is accessing it, for what purpose, whether it is accurate and how they can access it. This is particularly true where the transferred data is linked with personal information in other databases. Typically, through an electronic database, more public employees and more government agencies have more access to more information.

[23] Our recommendations with respect to data sharing focus on data sharing among public bodies in British Columbia. Concerns have arisen in the past about data sharing between government and the private sector but these are not discussed here. However, many of our recommendations should also apply to data sharing arrangements that government enters into with organizations outside government.

[24] There are valuable lessons to be learned from experiences other governments have had with privacy risks in data sharing and the expectations of the public in terms of privacy protection of their personal information. The issue of data sharing at the federal level came to the attention of the public when a database of Human Resources Development Canada (HRDC) was dismantled in May 2000 as a result of privacy concerns expressed by then Privacy Commissioner Bruce Phillips in his 1999–2000 Annual Report. The Longitudinal Labour Force File (LLLF) linked data from several social programs within HRDC, tax data from Canada Customs and Revenue Agency, and social assistance data from provinces and territories. It was used for research, evaluation, policy and program analysis to support departmental programs and services. Following an audit by his Office, the LLLF was characterized by the Commissioner as a de facto citizen profile because of its comprehensiveness, lack of transparency, indefinite retention period and lack of protective legal framework. When the story broke, more than 60,000 people demanded access to their files.

[25] In a stated effort to improve service delivery outcomes, government is moving forward with a number of programs that involve widespread linking and disclosure of personal information within government and across government agency boundaries. Recent examples include the provincial Electronic Health Record project, the Prolific Offender Management Pilot, Downtown Community Court, the Homelessness Intervention Project and the Integrated Case Management System. While the value of information sharing within and across government to achieve improved service delivery and efficiency is recognized, it is a value that must be properly balanced against legitimate expectations of privacy.

THE PUBLIC MUST BE ENGAGED IN DISCUSSIONS AROUND REDUCING PRIVACY RIGHTS TO FACILITATE DATA SHARING

[26] Privacy is often, and wrongly, in our view, seen as a "barrier" by government entities to "efficient and effective" service delivery. Government agencies often suggest that the privacy protections contained in FIPPA be weakened to allow for liberal sharing of citizen personal information, within and across government entities. We are adamant that no legislative amendments to FIPPA are needed to authorize data sharing and data matching activities within government, and would strongly oppose any weakening of the existing right to privacy.

[27] Existing provisions provide sufficient authority for government data-sharing activities and set minimum conditions that are appropriate and reasonable. For example, s. 33.2(d) of FIPPA provides a significant degree of support and flexibility for data sharing in relation to a common or integrated program or activity between public bodies. It reads as follows:

> 33.2 A public body may disclose personal information referred to in section 33 inside Canada as follows: …
>
> (d) to an officer or employee of a public body or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties of the officer, employee or minister to whom the information is disclosed;

[28] Government must establish a formal structure for that common or integrated program or activity through such means as memoranda of understanding or information-sharing agreements that support the program or activity. They should document the purpose for the disclosure of personal information and how that personal information will be protected.

[29] Section 35 of FIPPA permits the disclosure of personal information for the purpose of research, including research to assess the needs of citizens and the efficacy of government services they are receiving if the following conditions are met:

> 1 the research purpose cannot be accomplished with de-identified data;
>
> 2 that any record linkage is not harmful;
>
> 3 that the head of the public body has approved conditions relating to security and confidentiality; removal or destruction of individual identifiers; and subsequent disclosures; and
>
> 4 that information-sharing agreements have been signed.

[30] What is needed at this time, however, is a code of practice that sets out the privacy obligations of public bodies in the conduct of their data sharing projects. This code of practice would ensure that privacy protection is embedded into the design of all data sharing projects.

[31] The code of practice should be developed by government in an open and transparent manner with stakeholder consultation through something like a White Paper process. The OIPC should review and approve the code of practice once it is drafted. A code of practice developed by government that is approved by the OIPC would be an integral part of the appropriate balance needed to achieve both appropriate data sharing and privacy protection.

[32] A public consultation process on data sharing was successfully conducted by government and the Commissioner's office in Britain in recent years. In October 2007, following extensive public consultation on the government's proposals, the U.K. Information Commissioner issued a comprehensive

"Framework Code of Practice for Sharing Personal Information"[7] providing guidance on adherence to fair information practices in the sharing of personal information by organizations. The Code was reviewed in 2008 and recommendations were made to entrench it in law. The Ministry of Justice agreed with these recommendations and described the two primary purposes of the Code as being (1) to provide practical guidance to the public and (2) to promote good practice in the sharing of personal data. It committed to a new statutory requirement that would require the Information Commissioner to develop a code on the sharing of personal data that would be approved by Parliament. The work done in the U.K. had a successful outcome for both privacy and data sharing. A public consultation process resulting in a code of practice with the involvement of the Information Commissioner is a blueprint that British Columbia should follow. A clear and authoritative role for the OIPC is an essential outcome.

Recommendation #2:

Government should not proceed with any more data sharing initiatives until a meaningful public consultation process has occurred, and the outcome of that process is an enforceable code of practice for data sharing programs.

A GOVERNMENT CHIEF PRIVACY OFFICER IS NEEDED

[33] In British Columbia, a government-appointed Chief Privacy Officer is urgently required to act as a privacy advocate in the decision-making process and to ensure that privacy is fully considered and respected in any new initiative. Former Commissioner David Loukidelis recommended that Government should establish the senior executive level position of Chief Privacy Officer. Most recently, the Acting Commissioner's investigation report into the privacy breach involving the Ministry of Housing and Social Development and the Ministry of Children and Family Development made the same recommendation.[8] Given the increased likelihood and scope of a privacy or security breach in a data sharing initiative, it is even more incumbent on government to create a senior executive level position of Chief Privacy Officer to lead the development of a framework code of practice and nurture a culture of privacy among those involved in data sharing initiatives.

---

[7] Accessible at www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf.

[8] Accessible at: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF10-01.pdf.

[34] The Chief Privacy Officer could oversee the public consultation process and be responsible for implementing a data sharing code of practice once it has been approved by the OIPC.

Recommendation #3:

A Government Chief Privacy Officer should be appointed.

DATA SHARING INITIATIVES MUST BE JUSTIFIABLE AND APPROVED BY THE INFORMATION AND PRIVACY COMMISSIONER

[35] FIPPA currently allows the Information and Privacy Commissioner to "comment on anything that affects access and privacy rights" but does not require public agencies to disclose any proposals that may raise privacy concerns, including large-scale data sharing initiatives. There should be an explicit oversight role for the OIPC with respect to reviewing and approving data sharing arrangements between ministries. Efforts made at the federal level to require review of data sharing proposals by the Privacy Commissioner without legislative authority have not been successful and are illustrative of the problems that can arise in introducing an oversight role by policy only. In 2006, the Privacy Commissioner of Canada suggested that data-matching guidelines be legislated. Government departments rarely notified her office of information-matching programs and many managers involved in data-matching programs appeared to be unaware of the policy.

[36] There are precedents set across the world for this type of oversight. Australia and New Zealand allow data sharing only with prior authorization of the Commissioner. Under the New Zealand *Privacy Act*, government can engage in data matching only with the prior authorization of the country's privacy commissioner.

Recommendation #4:

FIPPA should be amended to give the OIPC a statutory mandate to review and approve all data sharing initiatives.

GOVERNMENT RESEARCH MUST MEET PROPER RESEARCH STANDARDS

[37] Some form of specific ethics review is necessary and desirable for government's data sharing activities for the purposes of research. Complementary research-governance measures should be adopted in addition to the approval role for the OIPC.

[38] Researchers at universities or hospitals must have their research proposals approved by a Research Ethics Board in order to receive funding and access to personal information. These boards are appointed by such institutions to review research proposals to ensure that the risks of research are reasonable and proportionate to the potential contribution of the research to the advancement of knowledge. This requirement applies to the secondary use of personal information for research. The Tri-Council Policy Statement of the federal Interagency Advisory Panel on Research Ethics provides guidance to Research Ethics Boards in terms of factors that should be considered, including that identifying or identifiable information is essential to the research and that appropriate measures will be taken to protect the privacy of the individuals and to ensure the confidentiality of the data. These conditions are similar to those found in s. 35(1) of FIPPA.

[39] In British Columbia, the *E-Health (Personal Health Information Access and Protection of Privacy) Act* ("E-Health Act") prohibits disclosure of personal information from a health information bank for research or planning purposes unless the arm's length Data Stewardship Committee established under the E-Health Act approves. The committee may approve the disclosure only if certain criteria are met. These criteria are essentially the same as those found in s. 35(1) of FIPPA. An analogous committee with a statutory mandate to approve research requests for PharmaNet data (PharmaNet Stewardship Committee) has been functioning for over 10 years.

[40] Consistent with this statutory and policy direction, a committee of experts should be appointed by government that would function in a manner similar to Research Ethics Boards and the stewardship committees of the Ministry of Health Services. This committee would apply the criteria in s. 35(1) of FIPPA and such other criteria as are considered desirable in the committee's terms of reference. Committee members should represent an appropriate range of interests, including government officials, researchers and privacy advocates. The committee's approval should be a mandatory pre-condition to disclosure of personal information by any public body for research purposes. The accountability and transparency thus provided will go a long way to reassuring public bodies, and the public, about government's research activities.

Recommendation #5:

Amend FIPPA to require that data sharing projects for the purpose of research must be subject to ethics review by an arm's length data stewardship committee.

PRIVACY IMPACT ASSESSMENT ON NEW SYSTEMS SHOULD BE LAYERED

[41] It is often said that privacy must be "baked in" to electronic file management systems ("databases"), including data sharing initiatives. New information technologies create a large appetite to collect, use, link and disclose "honey pots" of data, and therefore it is necessary to impose a requirement on planners to use a privacy lens at all phases of the project. This is most effectively done through the tool of the privacy impact assessment.

[42] A privacy impact assessment is a tool that requires public bodies and organizations to identify privacy risks in the collection, use, and disclosure of personal information and their strategies to mitigate them. There is a requirement in FIPPA for privacy impact assessments to be conducted by ministries of government [s. 69(3)].

[43] In our recent three-year investigation of a health authority database we discovered that while the health authority had voluntarily completed a privacy impact assessment, the assessment did not evaluate the project at each of the conceptual, design and implementation phases.[9] The system we evaluated had numerous fundamental privacy flaws that would have been identified had privacy impact assessments been completed at each of the key phases of the project. Based on this intensive investigation and on the knowledge that health authorities are responsible for some of the most sensitive personal information of British Columbians, we are of the view that health authorities should be required to complete privacy impact assessments.

[44] Another major government project is the Integrated Case Management System. This is the system announced in the recent throne speech. We have been advised that despite the fact that plans to purchase a system began at least two years ago and in fact the system has been purchased, no privacy impact assessment has been completed.

[45] It should be specified in FIPPA that privacy impact assessments must be completed at the conceptual, design, and implementation phases of databases. This requirement should be extended to health authorities because they use databases containing very sensitive personal information to a significant degree.

Recommendation #6:

Add a requirement in FIPPA that privacy impact assessments must be completed at the conceptual, design and implementation phases of an electronic record project. This requirement should apply to health authorities as well as to ministries of government.

[9] http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF10-02.pdf.

C. IMPROVING ACCESS IN THE 21ST CENTURY

ELECTRONIC READING ROOMS—ANOTHER CALL FOR ROUTINE PRO-ACTIVE DISCLOSURE

[46] In our 2008 report, *"Timeliness of Government's Access to Information Responses: Report for Calendar Year 2008"*[10] we examined government's performance in responding to access to information requests. Only 4 of 22 ministries actually had an average processing time within the statutory 30-day time limit.

[47] Former Commissioner Loukidelis noted that,

> For over a decade now, successive administrations have failed to tackle the chronic problem of delay in provincial government ministry responses to access to information requests under the Freedom of Information and Protection of Privacy Act. My attempts, and the attempts of the OIPC staff over more than a decade to advocate for change and resolve the challenge of delay have not succeeded overall.[11]

[48] As a result we made a series of recommendations to improve access, including pro-active disclosure where:

> The public body actively and regularly publishes, without formal access requests, records of interest to the public. This is known as routine release or pro-active release of records. At the very least, records such as program audits, financial audits, impact assessments, records previously released in response to access requests will be posted on the internet and otherwise made available as part of a well-functioning routine release process. As part of a successful disclosure program, program area staff should regularly review their records for posting and staff should be encouraged to identify records for pro-active release.[12]

[49] Routine disclosure could reduce the costs of freedom of information by avoiding the necessity of responding individually to specific and often repeated access requests for the same information, and enhance openness. The benefit of implementing routine disclosure goes beyond easier public access to information: reports by participating public bodies have indicated that the initial investment is repaid through a reduction in access request processing costs.

---

[10] http://www.oipc.bc.ca/investigations/reports/F08-35580_Calendar_2008_Report_Card (Feb_2009).pdf.
[11] http://www.oipc.bc.ca/investigations/reports/F08-35580_Calendar_2008_Report_Card (Feb_2009).pdf at p. 5.
[12] http://www.oipc.bc.ca/investigations/reports/F08-35580_Calendar_2008_Report_Card (Feb_2009).pdf at p. 18.

[50] We are not alone in calling for the practice of routine disclosure. For example, in a 2002 mandated review of Québec's *Access Act*, Jennifer Stoddart, then-President of the Commission d'accès à l'information and now Canada's Privacy Commissioner, advocated broad reforms to Québec's access to information system. She wrote, "At the beginning of this new century, the right to know is recognized as a basis and a prerequisite for the exercise of other rights in a democracy. From now on, it is the state, in all its forms, that must make information accessible to citizens, without their having to take the initiative."[13]

[51] The practice of routine disclosure has been adopted at the federal level. The federal *Access to Information Act* has a mandatory publication scheme requiring certain information be made publicly available on a routine basis. Ministers must publish, at least annually, a description of each ministry's responsibilities, the records and information for which the ministry is responsible and contact information for the officer in charge of that information. Bulletins updating these ministerial responsibilities must be issued at least twice each year.

[52] An amendment to FIPPA is needed to require electronic disclosure of information that has been requested and is likely to be requested again. This is admittedly a reactive approach to routine disclosure, since the obligation to routinely disclose is only triggered after at least one access request is made for records that may be subject to further requests.

[53] The current U.S. administration recently strengthened its commitment to proactive disclosure. On his first day in office in January 2009, President Barack Obama issued a memorandum to heads of government departments and agencies advising that routine disclosure should be the norm. A U.S. Department of Justice post reported on January of 2010, that Mr. Obama, called on agencies to "adopt a presumption in favour of disclosure and to apply that presumption to all decisions involving [the] FOIA." This presumption of disclosure includes taking "affirmative steps to make information public, and utilizing modern technology to inform citizens about what is known and done by their Government."[14]

[54] The type of information that should be made routinely available would include factual material, statistical surveys, public opinion polls, environmental impact statements and other records often of interest to the public.

[55] We made similar recommendations to the 2004 Special Committee, who agreed, and made the following recommendations:

---

[13] Report on the implementation of the Access Act and the Private Sector Act – Summary, "Reforming Access to Information: Choosing Transparency." (November, 2002), p. 4.

[14] *United States Department of Justice Office of Information Policy FOIA Post: Creating a New Era of Open Government*. (April 2009). www.justice.gov/oip/foiapost/2009foiapost8.htm.

> **Recommendation No. 5: Add a new section at the beginning of Part 2 of the Act requiring public bodies – at least at the provincial government level – to adopt schemes approved by the Commissioner for the routine disclosure of electronic records, and to have them operational within a reasonable period of time.**
>
> **Recommendation No. 12: Amend section 13(2) to require the head of a public body to release on a routine and timely basis the information listed in paragraphs (a) to (n) to the public.**

[56] The records listed in s. 13(2)—factual material, statistical surveys, public opinion polls, environmental impacts statements—are certainly the types of records of significant interest to the public.

[57] The two recommendations have been "under consideration" by government for six years.

Recommendation #7:

Add a new section at the beginning of Part 2 of the Act requiring public bodies to adopt schemes approved by the Commissioner for the routine disclosure of electronic records, and to have them operational within a reasonable period of time.

REQUIREMENT TO PROVIDE ELECTRONIC COPIES

[58] Public bodies should be required to use information technology to facilitate efficient and cost-effective responses to access requests.

[59] Section 9(2) of FIPPA provides that a public body must disclose a copy of a record where the applicant has asked for a copy and the record can reasonably be reproduced. However, most public bodies maintain their records electronically. Disclosure of electronic records in electronic form assists applicants by reducing cost and improving timeliness of responses. Electronic documents could be released as email attachments, CDs or on thumb drives.

[60] In 1996 amendments were made to the U.S. federal *Freedom of Information Act*. The House of Representatives' report on the amendments noted these benefits to disclosure in electronic form:

> [T]he information technology currently being used by executive departments and agencies should be used in promoting greater efficiency in responding to FOIA requests. This objective includes using technology to let requestors obtain information in the form most useful to them.

> Existing technologies for searching electronic records can often review materials more quickly than is possible via a paper review. Harnessing these tools for FOIA can enhance the operation of the Act.

[61] Legislation in Nova Scotia and P.E.I. treat providing electronic records as part of the duty of public bodies to assist applicants with their requests. For example, s. 8(2) of Nova Scotia's *Freedom of Information and Protection of Privacy Act* provides:

> (2) The head of a public body may give access to a record that is a microfilm, film, sound recording, or information stored by electronic or other technological means by
>
> (a) permitting the applicant to examine a transcript of the record;
>
> (b) providing the applicant with a copy of the transcript of the record;
>
> (c) permitting, in the case of a record produced for visual or aural reception, the applicant to view or hear the record or providing the applicant with a copy of it; or
>
> (d) permitting, in the case of a record stored by electronic or other technological means, the applicant to access the record or providing the applicant a copy of it.

[62] Similarly, in the United States, the Washington State Court of Appeals recently found that a public body was obligated to provide emails concerning public business in electronic form, rather than in print, to an applicant. In fact, in the interests of making records more easily accessible, U.S. federal public agencies have been required since 1996 to produce and store records in electronic form.

[63] We recommend an amendment to FIPPA requiring that, where a record exists in electronic form and a public body can reasonably provide it in that form, it should release the record in electronic form.

Recommendation #8:

Amend s. 9(2) of FIPPA to require that public bodies release records in electronic form where the record can reasonably be reproduced in electronic form.

BETTER ACCOUNTABILITY FOR THE CREATION AND DESTRUCTION OF RECORDS

[64] The OIPC has investigated hundreds of complaints concerning the fact that a requested record does not exist, as one was never created. Former Commissioner Loukidelis believed that a duty to document should be introduced in British Columbia. He stated:

> I have recommended in the past that there be a legislative duty to document here in British Columbia – not, I would argue, an onerous one by any means, but some duty on the part of public servants to record actions and decisions and reasons therefore. One can control this by prescribing certain criteria that would surround the extent of it. Again, if you were making a policy decision or taking a decision to embark on a program or cancel it, it seems to me there should be some duty to document. This is not just a question of creating records for the purposes of openness and accountability. One could argue, and I do argue, that it is a question of good governance and good government operation, and it fits into this larger context that I believe archivists and librarians and others are deeply concerned about in relation to the information management and information holdings of governments across the country, and to the state of information management legislation and practice here in Canada.[15]

[65] Other suggestions on this topic include that a "duty to document" be contained in access to information legislation, which would include a requirement for detailed documentation of key government actions and decisions, and an obligation to keep records up to date and readily retrievable, with penalties for non-compliance.[16] A duty to document key government decisions is critical to good governance.

[66] Inappropriate destruction of records is an ongoing concern and a threat to accountable government. In at least three Canadian jurisdictions,[17] the Commissioner has legislative authority to investigate and ensure compliance with rules relating to the proper destruction of records. At this time, no such power exists within FIPPA.

[67] For example, the Alberta *Freedom of Information and Protection of Privacy Act* states:

> 3 This Act
>
> **...**
>
> (e) does not prohibit the transfer, storage or destruction of a record
>
> (i) in accordance with an enactment of Alberta or Canada
>
> ...

---

[15] Standing Committee on Access to Information, Privacy and Ethics, David Loukidelis, March 11, 2009 (1700).

[16] Standing Committee on Access to Information, Privacy and Ethics, Ken Rubin, April 1, 2009 (1555).

[17] In Alberta, see ss. 3(e) and 53(1)(a) of the *Freedom of Information and Protection of Privacy Act*, Chapter F-25. In Manitoba, see ss. 3(b) and 49(a) of the *Freedom of Information and Protection of Privacy Act*, c. F175. In Prince Edward Island, see ss. 3(e) and 50(1)(a) of the *Freedom of Information and Protection of Privacy Act*, Chapter F-15.01.

> 53(1) In addition to the Commissioner's powers and duties under Part 5 with respect to reviews...the Commissioner may:
>
> (a) conduct investigations to ensure compliance with any provision of this Act or compliance with rules relating to the destruction of records
>
> (i) set out in any other enactment of Alberta
>
> (ii) 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,

[68] In British Columbia, the *Document Disposal Act* sets requirements for legislative approval for disposition of government information and requirements for applying approved scheduled retention periods and final dispositions to recorded information. The OIPC has no power to investigate and ensure compliance with the *Document Disposal Act*.

[69] The right of access can only be exercised if a record exists. The ability to investigate the destruction of records is a natural extension of the jurisdiction of the OIPC. This should include the power to ensure that electronic records are properly managed according to legislative retention schedules.

[70] Public bodies must create and adhere to robust policies that ensure the appropriate classification, storage and destruction of electronic records, because it is in electronic records that much of the daily life and memory of an organization is recorded.

Recommendation #9:

(a) Amend FIPPA to give the Commissioner the power to investigate and ensure compliance with the *Document Disposal Act* or compliance with rules relating to the destruction of records.

(b) Add to FIPPA a "duty to document" key prescribed government decisions.

STRENGTHENING DISCLOSURE IN THE PUBLIC INTEREST

[71] Section 25 of FIPPA requires the head of a public body to disclose, without delay, information about a risk to the environment or the health and safety of the public, regardless of whether a request for information has been made. We believe the wording of this section is too narrow to have any real impact.

[72] The terms "without delay" indicate that the duty to disclose records in the public interest only materializes in the event of an urgent or compelling risk. This section cannot be used to require the disclosure of records that have significant public interest, such as reports addressing how a public authority dealt with a public health issue.

[73] The legislative criteria for release of records in the public interest must be broadened, to mandate the disclosure of non-urgent information that nevertheless concerns a matter of clear public interest.

[74] There are many examples to follow. The Cayman Islands' *Freedom of Information Law* (2007) has a notwithstanding provision saying that, despite exemptions articulated in the law, access to information will be granted if it "would nevertheless be in the public interest."[18] All exemptions to disclosure in the Ireland access law are subject to a "public interest test." This test "requires consideration to be given to whether the public interest in disclosure of a particular record is better served and outweighs the potential harm or injury arising from such disclosure."[19]

[75] The amended s. 25 would continue to apply despite any other provision of the Act. That is, it would override exemptions, where disclosure was deemed to be in the public interest, and where the benefit of disclosure was considered to be greater than any potential harm.

Recommendation #10:

Amend s. 25 to require pro-active disclosure despite any other provision of FIPPA where there is a significant public interest in the disclosure that outweighs any potential harm from the disclosure.

FIPPA MUST APPLY TO RECORDS OF CONTRACTORS AND CORPORATE ENTITIES CREATED BY PUBLIC BODIES

[76] Section 3 states that FIPPA generally applies to records "in the custody or under the control of a public body." In 2004, we recommended that FIPPA be expanded to apply to records created by, or in the custody of an external service provider in the course of carrying out contractual duties for a public body. These records should remain in the custody or under the control of the

[18] *The Freedom of Information Law* (2007) www.foi.gov.ky/pls/portal/docs/PAGE/FOIHOME/DOCLIBRARY/FOILEGISLATION/FREEDOM%20OF%20INFORMATION%20LAW%2C%202007.PDF.

[19] *A Short Guide to FOI Acts*, n.d. http://www.foi.gov.ie/short-guide-to-the-foi-acts/chapter-4-exemptions/.

contracting public body. To date this recommendation has not been implemented.

[77] As government continues to outsource services and functions still paid for by the taxpayers of British Columbia, this amendment is urgently required. This recommendation is needed to clear up any confusion on the part of contractors and public bodies regarding who has custody or control of requested records.

[78] Recently the British Columbia Supreme Court held that records of an incorporated company, wholly owned by Simon Fraser University (SFU), were not under the control of SFU for the purposes of FIPPA.[20] The company involved was created by SFU and staffed by SFU employees, with the apparent intent to operate it as a holding company to promote SFU's commercial interests. This decision is under appeal.

[79] We note that similar facts to those found in the SFU decision have arisen in the context of local government bodies, such as municipalities, who have created a separate corporation to engage in a business pursuit.[21] In the case of a local government body however, these companies would be considered to be public bodies in their own right due to the definition of *local government body* in Schedule 1 of FIPPA which includes "(n) any board, committee, commission, panel, agency or corporation that is created or owned by a body referred to in paragraphs (a) to (m)[22] and all the members or officers of which are appointed or chosen by or under the authority of that body." This definition does not apply to entities that SFU owns however as SFU is defined as an *educational body* rather than a *local government body* in FIPPA.

[80] The principle of transparency and accountability requires that a corporation, or other organization created by a public body to promote its interests, be subject to the same obligations under FIPPA as the public body itself. In addition, there is no clear policy reason why a wholly owned corporation

---

[20] *Simon Fraser University v. British Columbia (Information and Privacy Commissioner) 2009 BCSC 1781.* This decision is currently being appealed by the OIPC.

[21] For a recent example see OIPC order F09-08 where the Village of Burns Lake incorporated a company to engage in a community forest enterprise. The company was considered to be a public body in its own right under FIPPA as a result of paragraph (n) of the definition of *local government body,* as it had been created by the Village and all its officers had been appointed by the Village. Available at http://www.oipc.bc.ca/orders/2009/OrderF09-08.pdf.

[22] Paragraphs (a) to (m) list a municipality; a regional district; an improvement district as defined in the Local Government Act; a local area as defined by the Local Services Act; a greater board as defined in the Community Charter; a board of variance established under the Local Government Act or the Vancouver Charter; the trust council, executive committee, local trust committee and trust fund board of the Island Trust; The Okanagan Basin Water Board; a water users' community as defined in the Water Act; the Okanagan-Kootenay Sterile Insect Release Board; a municipal police board established under the Police Act, and; a library board as defined in the Library Act.

of a local government body should be subject to FIPPA while a wholly owned corporation of an educational body should not.

[81] To that end we recommend that paragraph (n) of the definition of *local government body* be removed and added to the definition of *public body* in Schedule 1. This would broaden that provision with the result that any board, committee, commission, panel, agency or corporation that is created or owned by a public body would be a public body in its own right and subject to FIPPA.

Recommendation #11:

(a) Amend FIPPA so that paragraph (n) of the definition of local government body is moved into the definition of public body in Schedule 1.

(b) Amend s. 3 should be amended to clarify that records created by or in the custody of a service-provider under contract to a public body are under the control of the public body on whose behalf the contractor provides services.

IMPROVE ACCESS TO ONE'S OWN PERSONAL INFORMATION

[82] FIPPA gives individuals "a right of access to, and a right to request correction of, personal information about themselves." In 2004 we recommended that FIPPA require public bodies make available to an individual his or her own personal information without the need of a formal access request and free of charge.

[83] The 2004 Special Committee agreed, recommending:

> **Recommendation # 26: Amend section 71 to require public bodies to make available to an individual his or her own personal information free of charge and without an access request, but subject to any access exceptions under the Act.**

[84] This recommendation remains "under consideration" by government.

[85] Access to information through a formal process should be a last resort needed only where documents require a line by line review to ensure that no exceptions to disclosure apply. Where a public body has created records that contain only the personal information of the applicant, there is no reason for the public body to require that a request for such a record by the individual go through a formal access process. The formal access process is time consuming and resource intensive for the public body.

[86] We noted in our 2004 submission that some public bodies in British Columbia—the Workers' Compensation Board is a good example—have taken the initiative of providing their clients with routine access, free of charge, to their own personal information. Where the personal information is subject to exceptions under FIPPA, the public bodies divert only that information to the formal freedom-of-information stream for treatment under the Act. This practice recognizes that individuals have a right of access to their own personal information and that in many cases their information may be released routinely, without an access request.

Recommendation #12:

Amend section 71 of FIPPA to require that public bodies make available to an individual his or her own personal information free of charge and without an access request, but subject to any access exceptions under the Act.

WHO CAN ACT FOR OTHERS

[87] There are times when individuals such as minors and incapable adults are not able to make access requests or privacy complaints on their own. Section 3 of the FIPPA Regulation prescribes who may act for minors, for individuals with committees and for deceased individuals. It does not recognize that individuals may have other types of legitimate representatives, such as those with power of attorney or representatives under the *Representation Agreement Act*. It also does not rank nearest relatives in order of priority and does not define "spouse".

[88] By contrast, ss. 1 to 4 of the PIPA Regulation provide a comprehensive guide to determining who the nearest relative is, who may act for minors and other types of representatives who may act for individuals, as well as defining "spouse".

[89] Section 3 of the 1993 FIPPA Regulation should be updated to add authorized representatives, such as those with the power of attorney, to the existing list of persons who may act for others. This would reflect current policy and avoid potential confusion arising from the inconsistency between FIPPA and PIPA in this regard.

[90] The 2004 Special Committee made a recommendation supporting this objective as follows:

Recommendation #28: Amend section 3 of the 1993 *Freedom of Information and Protection of Privacy Regulation* to make it consistent with sections 1 to 4 of the *Personal Information Protection Act*.

[91] This recommendation is still "under consideration" by government.

[92] This is a straightforward recommendation that would make FIPPA consistent with PIPA. It would allow properly appointed representatives to ensure that individuals can take advantage of their access and privacy rights under both PIPA and FIPPA and it would provide clarity in terms of the order of priority of "nearest relatives".

Recommendation #13:

Amend s. 3 of the 1993 FIPPA Regulation to make it consistent with ss. 1 to 4 of the PIPA Regulation.

A RIGHT TO ANONYMITY

[93] One of the findings of our 2009 Timeliness Report was the fact that the identity of an applicant had a significant negative impact on how quickly the request was processed. For example, 94% of requests made by public bodies were processed on time, 82% of requests by other governments were on time, and 74% of requests made by individuals were on time. However only 49% of media responses were on time in 2008, 53% of responses to political parties were on time and 57% of interest group responses were on time. This trend has been consistent for the past decade.

[94] Although there is no provision in FIPPA that prohibits an applicant from making an anonymous request, we believe this should be a right in law. In our view, applicants and complainants should have the right to anonymity, and the power to decide whether their identity should be made known. This was a concern raised by other witnesses during the 2004 FIPPA review consultation process who objected to their names being disclosed in email communications among public bodies, without their consent.

[95] Timely access to information should not be affected by the nature of the request or the identity of the requester. The legislation does not require requesters to provide reasons for making an access request. A person's motives for making a request are irrelevant and a response to an access request should not be influenced by whether the requested information is for the benefit of one person or of an organization or group the applicant represents.

[96] The most efficient way to ensure that all requests are treated equally is to guarantee that the identity of the requester remains shielded throughout the process, known only to the branch responsible for making the decision on disclosure and for sending the records to the requester. Practices vary across ministries around concealing or revealing the identity of a requester throughout the sign-off process. There is no valid operational reason for communicating the identity of the applicant to any executive, program area, records managers, sign-off authorities or public affairs officers in the response process.

[97] Obviously, anonymity cannot be guaranteed when the request is for personal information. Even so, in these cases, to ensure timeliness and protect the privacy of the requesters, the response processes should, wherever possible, protect anonymity. The same is true where other third-party information, such as business information that may be protected under s. 21, is involved.

[98] An excellent example of the right to anonymity is the following provision contained in the Finland Act, Openness of Government Activities.

> The person requesting access need not identify himself/herself nor provide reasons for the request, unless this is necessary for the exercise of the authority's discretion or for determining if the person requesting access has the right of access to the document.[23]

[99] The 2004 Special Committee made the following recommendation:

> **Recommendation #6: Amend section 4(1) to establish that an applicant who makes a formal access request has the right to anonymity throughout the entire process.**

[100] As with many other recommendations made by the Special Committee, this has not been implemented.

Recommendation #14:

Amend section 4(1) to establish that an applicant who makes a formal access request has the right to anonymity throughout the entire process.

EXCEPTIONS TO DISCLOSURE

[101] We devote a large portion of our resources, from mediation through to inquiry, to the review of decisions by public bodies to deny access to information. For the most part, our experience is that the exceptions to disclosure in FIPPA work well and are consistent with exceptions to disclosure in other access

[23] Section 13(1); accessible at http://www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf.

legislation across Canada. Indeed, a review of our orders over the last few years confirms that public bodies are generally applying exceptions properly. Our one major area of concern remains s. 13 – the discretionary exception that allows public bodies to withhold policy advice or recommendations. We also have two minor recommendations that would simply help FIPPA work better.

Restore access rights removed by the Courts

[102] Section 13(1) is a discretionary class-based exception permits a public body to withhold information that would reveal advice or recommendations developed by or for a public body or a Minister. The exception is intended to be narrow and does not extend to background information on which the advice or recommendations are based. Among other things, s. 13(2) specifically provides that s. 13(1) cannot be applied to any factual material, a public opinion poll or a statistical survey.

[103] An interpretation of s. 13(1) by the British Columbia Court of Appeal in 2002[24] broadened the exception by interpreting "advice" to include an opinion that involves exercising judgment and skill to weigh the significance of matters of fact, including expert opinions on matters of fact on which a public body must make a decision for future action. The problem is that withholding expert opinions on matters of fact undermines the requirement to disclose factual material in s. 13(2). A number of our orders since 2002 have involved the application of s. 13(1) and its frequent use, often for information of a routine nature or for information that would illuminate government decision-making, is of concern to us.

[104] Because of this court decision, s. 13(1) must be amended to re-assert the Legislature's original intention and assert the supremacy of the Legislature. As Attorney General in 1992, Colin Gabelmann presided over the framing and the unanimous passage of FIPPA. In speaking about this issue in 2007 at the British Columbia Information Summit, he eloquently affirmed the Legislature's original, and clear, intention in passing s. 13(1). He characterized the Court of Appeal's interpretation of s. 13(1) as an "astonishing perversion" that has resulted in "reversal of the Legislature's intention, as originally expressed in the Legislature and in the Act." He described the present state of affairs as an "outrage" that must be remedied.

[105] Given his key role as a legislator and as the minister responsible for the drafting and passage of the law, the rest of Mr. Gabelmann's remarks about s. 13(1) merit extensive quotation and should be given the greatest possible weight:

---

[24] *College of Physicians and Surgeons of British Columbia* v. *British Columbia (Information and Privacy Commissioner),* [2002] B.C.J. No. 2779.

...we designed wording which struck a balance but ensured that government and its advisors would be able to conduct public business in a full, frank and informed manner.

The wording and intent was clear—at least we thought it was: in Section 13 "Policy Advice" permits an exception from access for "information that would reveal advice or recommendations developed by or for a public body or a minister". We meant that to mean—and I believe it does mean—that "advice or recommendations" was limited to those parts of documents or reports that advocated that Government choose a particular course of action or make a particular decision; in effect, "we recommend that you do this", or "we advise that you do that". Following that, we specified a long list of items which "the head of a public body must not refuse to disclose".

Section 13 was so clear and obvious that there was not a word spoken by any member of the House on it during the Committee stage debate. Not a word!

...I have to tell you that the Appeal Court quite simply failed to understand our intention–the intention of the Legislature—when using these words as we did. We were attempting to use plain language as much as possible in Legislation and the words "advice and recommendations" have some pretty plain and clear, and needless to say, dictionary meanings which the Appeal Court seems to have rejected. It has become so ridiculous now that a technical report on the state of British Columbia Place stadium can be almost entirely blacked out because of the Court's misreading of the intent of the Legislature in 1992. The Act required that factual material must be released; advice or recommendations to Cabinet would not be released. So now we have the bizarre situation where reports are not released—reports which are specifically defined in the legislation as reports which must be released! I can't think of another example where the Appeal Court got something as wrong as they did here. The Act should not really have to be amended because it is really clear in every way, but unfortunately an amendment has been our only option for the past five years. A government which believes in freedom of information would have introduced amendments in the first Session of the Legislature after that Appeal Court decision to restore the Act's intention.

Now, the Appeal Court decision means that the secrecy advocates in government are using the two sections of the Act in tandem to refuse to allow public access to material that is at the very heart of the principles of freedom of information. This is an outrage and must be remedied.

It is gratifying that the second mandated review of the Act (which happened three years ago) resulted in a unanimous view of the Special Legislative Committee that Section 13 should be amended to restore the original meaning of the words, so that public servants and Ministers cannot hide behind that shameful Appeal Court decision. MLA Blair Lekstrom, who I believe is here today, chaired the Committee. He and the Committee understood the issue and are to be sincerely commended for including such a strong recommendation to fix the huge loophole created by the Court.

> What is not gratifying, however, is that in the five years that the government has had to introduce remedial legislation, it has failed to act. I trust that the Gordon Campbell who spoke so eloquently in 1998 will ensure that these and other amendments restoring the public's right to know in a timely fashion will be introduced in the Legislative Session which begins in a few days. However, I doubt that amendments are forthcoming. No doubt senior public servants, as well as the government are only too happy to have the law kept in its current state.
>
> ...
>
> And you know, we don't just believe in it because it's a nice thing to do. We are talking about the very foundation of our democracy. Professor Donald Rowat, away back in 1965, put it very well: "Parliament and the public cannot hope to call the Government to account without an adequate knowledge of what is going on; nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view."[25]

[106] The dangers of the 2002 British Columbia Court of Appeal decision were avoided by the Ontario Court of Appeal in 2005, when it rejected our Court of Appeal's expansive interpretation. In a case where the Ontario government cited and relied heavily on our Court of Appeal's decision, the Ontario Court of Appeal concluded that the Ontario Information and Privacy Commissioner's interpretation[26] of "advice or recommendations" was reasonable and said this:

> The most fundamental principle of interpretation is that words must be understood in light of the context and purpose of the whole statute. The purposes of the statute are stated by s. 1 of the Act [Ontario's *Freedom of Information and Protection of Privacy Act*] to be
>
> 1. The purposes of this Act are,
>
> (a) to provide a right of access to information under the control of institutions in accordance with the principles that,
> (i) information should be available to the public,
> (ii) necessary exemptions from the right of access should be limited and specific, and
> (iii) decisions on the disclosure of government information should be reviewed independently of government; and
>
> (b) to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.
>
> In my view, the meaning of "advice" urged by the Ministry would not be consonant with this statement of purpose. The public's right to information would be severely diminished because much communication within

[25] Accessible at : http://www.opengovernment.ca.

[26] The Ontario Commissioner's interpretation of "advice or recommendations" is the same as that long adopted in British Columbia, including in Order 00-08.

> government institutions would fall within the broad meaning of "advice", and s. 13(1) would not be a limited and specific exemption. I conclude, in the words of the Divisional Court that "the Commissioner's interpretation complies with the legislative text, promotes the legislative purpose, and is reasonable."[27]

[107] The British Columbia Court of Appeal's decision failed to interpret s. 13 in light of the explicit accountability objective in s. 2(1) of FIPPA and therefore has compromised the accountability and openness promised by FIPPA. The appropriate balance between openness and government confidentiality must be restored by amending s. 13 at the earliest opportunity.

[108] It has been suggested that the 2004 Special Committee's recommendation would affect the operational efficiency of government, its ability to formulate policy and its ability to advise ministers. This assertion is unsupported by any evidence. Similar arguments have surfaced from time to time since access to information legislation came into effect across Canada in the 1980s and 1990s, but there is no evidence that freedom of information laws—which contain ample, appropriate protections for the necessarily confidential aspects of governance—adversely affect the ability of public servants or elected officials to freely discuss matters, formulate policy or make decisions.

[109] No one in British Columbia, certainly, has shown that the situation which existed for nine years before the Court of Appeal's 2002 decision in any way adversely affected the operations of government or other public bodies. The fact is that full and frank discussions of policy advice and recommendations occurred before the Court of Appeal's decision narrowed the public's right of access, and effective discussions of issues would continue in government after enactment of the remedial amendment. By contrast, as the 2004 Special Committee recognized, for the government not to amend s. 13(1) seriously undermines public accountability by allowing public bodies to possibly withhold broad swaths of information.

[110] Government has indicated that it has formulated policy to ensure that s. 13(1) is appropriately interpreted and applied. If that policy is intended to circumvent or merely mitigate the Court of Appeal's decision, it will not be enough. Amendment of s. 13(1) is the only realistic way to address the Court of Appeal's decision. Policy is not binding even if it is well known and understood. Further, provincial government policy can apply only to the provincial government—there are over 2,900 public bodies in British Columbia and provincial government policy would apply to few of them.

---

[27] *Ontario (Ministry of Transportation) v. Ontario (Information and Privacy Commissioner)*, [2005] 0.J. No. 4047 (leave to appeal denied [2005] S.C.C.A. No. 563.

[111] During the 2004 review, we recommended the following amendment to s. 13:

> Section 13(1) should be amended to clarify the following:
>
> (a) "advice" and "recommendations" are similar and often interchangeably used terms not sweeping separate concepts,
>
> (b) "advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process,
>
> (c) the "advice" or "recommendations" exception is not available for the facts upon which advice or recommended action is based,
>
> (d) the "advice" or "recommendations" exception is not available for factual, investigative or background material, for the assessment or analysis of such material, or for professional or technical opinions.[28]

[112] The 2004 Special Committee agreed and found "there is a compelling case, as well as an urgent need, for amending s. 13(1) in order to restore the public's legal right of access to any factual information. If left unchallenged, we believe the court decision has the potential to deny British Columbians access to a significant portion of records in the custody of public bodies and hence diminish accountability…."[29]

[113] The 2004 Special Committee made the following recommendation:

> **Recommendation #11: Amend section 13(1) to clarify the following:**
>
> **(a) "advice" and "recommendations" are similar terms often used interchangeably that set out suggested actions for acceptance or rejection during a deliberative process,**
>
> **(b) the "advice" or "recommendations" exception is not available for the facts upon which advised or recommended action is based; or for factual, investigative or background material; or for the assessment or analysis of such material; or for professional or technical opinions.**

[114] Again, the government did not act on the Committee's recommendation.

---

[28] Submission of the Information and Privacy Commissioner to the Special Committee to Review the Freedom of Information and Protection of Privacy Act, February 5, 2004, p. 19.

[29] Special Committee to Review the Freedom of Information and Protection of Privacy Act, *Enhancing the Province's Public Sector Access and Privacy Law* (Legislative Assembly of British Columbia, 2004). http://www.legis.gov.bc.ca/CMT/37thparl/session-5/foi/ reports/ Rpt-FOIPPA37-5.pdf, at p. 20.

Recommendation #15:

Section 13(1) should be amended to clarify the following:

(a) "advice" and "recommendations" are similar and often interchangeably used terms not sweeping separate concepts,
(b) "advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process,
(c) the "advice" or "recommendations" exception is not available for the facts upon which advice or recommended action is based,
(d) the "advice" or "recommendations" exception is not available for factual, investigative or background material, for the assessment or analysis of such material, or for professional or technical opinions.

Records available for purchase

[115] Section 3 provides that FIPPA does not apply to certain officials and public bodies or to documents such as those used to prepare for legal proceedings, or those used by post-secondary instructors to prepare teaching materials. In 2004, the OIPC recommended that s. 3 should be expanded to say that FIPPA also does not apply to records available for purchase by the public.

[116] Currently, the matter of records available for purchase is dealt with under s. 20(1)(a) of FIPPA, which reads:

> 20(1) The head of a public body may refuse to disclose to an applicant information
>
> (a) that is available for purchase by the public, or
>
> (b) that, within 60 days after the applicant's request is received, is to be published or released to the public.

[117] Legislation from Canada and beyond, including Saskatchewan, Nova Scotia, Newfoundland, Yukon and Australia state that records available for purchase are not covered by freedom of information legislation.

[118] FIPPA is intended be an avenue of last resort for accessing records that are not otherwise available to the public. If information or records are available for purchase, such material should not need a special request under FIPPA. Section 20(1)(a) is in effect redundant. It would, therefore, be more straightforward for FIPPA not to apply at all to material that is available for purchase. This end could be achieved by exempting any records available for purchase by the public. Therefore we support the 2004 Special Committee's recommendation and repeat it below.

Recommendation #16:

Repeal section 20(1)(a) and amend section 3(1) to state that the Act does not apply to records available for purchase by the public.

Availability of personal information after death

[119] The OIPC recommended and the 2004 Special Committee agreed that it is not an unreasonable invasion of third-party privacy to disclose the personal information of an individual who has been dead for over 20 years.

[120] That recommendation was not implemented by government.

[121] Section 22 of FIPPA requires public bodies to refuse access to personal information where its disclosure would be an unreasonable invasion of third-party privacy. Public bodies must first look to s. 22(4) which lists information the disclosure of which is not an unreasonable invasion of personal privacy, *e.g.* salaries of public officials. If the personal information falls into one of these categories it must be released.

[122] If the information does not fall within one of these categories, the public body must assess whether or not the disclosure of the personal information would be an "unreasonable invasion of personal privacy". Section 22(3) and s. 22(2) assist with this determination by providing lists of factors to consider. Public bodies are not limited to the list of considerations in ss. 22(2) and 22(3). The fact that the records relate to a deceased person is not currently listed as a consideration in s. 22.

[123] Public bodies frequently consider requests for access to personal information of deceased individuals. One of the factors they properly consider is the length of time the person has been dead. We believe that while the deceased have privacy rights, such rights may diminish with time.[30]

[124] In some jurisdictions the definition of "personal information" is limited to "recorded information about an identifiable individual, either living or deceased if the individual has been dead for over 20 years, other than contact information". Ontario[31] and Alberta,[32] as well as federal privacy legislation[33] contain this definition.

---

[30] See Order F07-20 at http://www.oipc.bc.ca/orders/2007/OrderF07-20.pdf.
[31] Accessible at www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm#s2s2.
[32] Accessible at http://foip.alberta.ca/legislation/act/index.cfm.
[33] Accessible at http://laws.justice.gc.ca/eng/P-21/page-2.html.

[125] Our experience in the past six years suggests that there will be occasions when the personal information of an individual deceased for 20 years could cause an unreasonable invasion of personal privacy. For example, if an infant or young child dies as a result of a violent crime, the disclosure of that information relating to the crime and cause of death may well still result in the unreasonable invasion of the personal privacy of that infant or young child, particularly as there will likely be living family members.

[126] Another consideration is the fact that s. 36 of the Act permits the disclosure of personal information for archival or historical purposes where the information is about someone who has been dead for 20 or more years or where the information is in a record that has been in existence for 100 or more years. There is no such time limit in s. 22 of FIPPA.

[127] For the sake of internal consistency with s. 36, to clearly define when a deceased individual's rights have diminished, and to continue to protect personal information in unusual circumstances, we recommend that s. 22(2) be amended to state that a relevant circumstance is that the personal information relates to an individual who has been dead for more than 20 years. Such an amendment would accurately reflect current OIPC decisions and would support public bodies in their current practice of evaluating the length of time since death as a relevant factor in determining whether or not disclosure of the personal information of the deceased is an unreasonable invasion of personal privacy.

Recommendation #17:

Amend s. 22(2) to state that the personal information of an individual who has been dead for over 20 years is a relevant consideration in determining whether the disclosure of the deceased's personal information would be an unreasonable invasion of personal privacy.

D. IMPROVING OIPC PROCESSES

[128] After 16 years of access and privacy oversight, we have identified a pressing need to create a unitary process within our office. We have also identified four other process changes that are required to address retrogressive court decisions or because our experiences dictate that changes are necessary.

STREAMLINING OVERSIGHT PROCESSES

[129] In 2004, the OIPC made a number of recommendations to the Special Committee intended to streamline complaint and appeal processes under FIPPA. The Special Committee accepted many of the OIPC's recommendations and since then, there have been various legislative amendments to improve our processes. Nonetheless, we remain concerned that our processes are inefficient and confusing to the public and to public bodies.

[130] Chiefly, FIPPA continues to treat "complaints" and "reviews" as separate types of appeals, and, depending on the nature of the issue, we must either treat the matter as a "review" that may proceed to an inquiry, or as a complaint, that does not proceed to inquiry. The distinction between the two is often blurry.

[131] FIPPA must be amended to combine all of the processes into a unitary process as was recommended by the 2004 Special Committee, specifically:

> **Recommendation 20: Amend the Act to combine the complaint process and the review and inquiry process – referred to in sections 42(2) and 52(1) respectively – into a unitary process for the Commissioner to investigate, mediate, inquire into and make orders about complaints respecting decisions under the Act or other allegations of non-compliance with the Act.**

[132] In 2008, the OIPC made a similar recommendation regarding a unitary process for the complaint and review processes to the PIPA Review Committee. The PIPA Review Committee supported the OIPC's "streamlining proposal because it would make the legislation more accessible and understandable to the general public."[34]

[133] Despite this, government has not acted to implement these important recommendations. Citizens of this province would benefit from an accessible, unambiguous and streamlined complaint, review and inquiry process under FIPPA. Amendments to FIPPA are necessary because the current status of Parts 4 and 5 results in unnecessary complexity, administrative burden, and real costs, for the individuals and organizations involved in processes under FIPPA.

---

[34] *Streamlining British Columbia's Private Sector Privacy Law* (2008), http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/reports/PDF/Rpt-PIPA-38-4-2008-APR-17.pdf.

Recommendation #18:

FIPPA should be amended 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.

SUPREME COURT OF CANADA DECISION AFFECTS ACCESS RIGHTS IN BRITISH COLUMBIA

[134] FIPPA gives the Information and Privacy Commissioner the mandate to investigate, inquire into and make orders concerning whether public bodies and organizations have properly applied the statutorily-specified exceptions to the legislated rights of access under each statute. This includes oversight of the proper application of solicitor-client privilege under s. 14 of FIPPA.[35] Assessment of the existence of a claimed solicitor-client privilege can require the Commissioner to examine the records in issue. The examination is done confidentially, solely for the purpose of verifying the existence of the privilege and only when necessary for that purpose alone.

[135] Section 44(1)(b) of FIPPA provides that the commissioner may make an order requiring a person to produce for the commissioner a record in the custody or under the control of the person. Section 44(2.1) further provides that if a person discloses a record that is subject to solicitor-client privilege to the commissioner, the privilege of the record is not affected by the disclosure.

[136] In a 2008 decision, *Canada (Privacy Commissioner)* v. *Blood Tribe Department of Health*,[36] the Supreme Court of Canada held that the Privacy Commissioner of Canada did not have a right to access solicitor-client documents to determine whether a claim by a public body to withhold them on the basis of solicitor-client privilege has been properly exercised under the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In the Court's view, that role is reserved for the courts unless there is clear and explicit language in legislation that permits a statutory official to "pierce" solicitor-client privilege. PIPEDA is a federal law that applies to private sector organizations in some provinces.

[35] Section 23(2)(a) of the *Personal Information Protection Act* gives an organization the same authority to withhold records subject to solicitor client privilege when responding to an individual's request for access to his or her own personal information in the control of the organization.
[36] [2008] 2 S.C.R. 574, 2008 SCC 44.

[137] The *Blood Tribe* decision is significant for the administration of both FIPPA and PIPA because it clarified how general legal principles governing solicitor-client privilege apply to the interpretation of provisions in legislation like FIPPA and PIPA that may affect solicitor-client privilege. The Supreme Court held that:

1. Solicitor-client privilege has a uniquely important status in our legal system and thus within the scheme of exceptions to disclosure in information and privacy legislation.

2. Legislative language that may result in incursions on solicitor-client privilege—including provisions for the confidential review of records for the purpose of verifying the existence of the privilege—must be interpreted restrictively. General, as opposed to explicit and precise, language in document-production provisions in access to information and privacy legislation will not be read to include records that are protected by solicitor-client privilege.

3. Adjudicative review to verify the existence of solicitor-client privilege is an incursion on the privilege that may only be done when necessary to fairly decide the issue.

[138] Following the *Blood Tribe* decision, the OIPC implemented a solicitor-client privilege case review process that is separate from the standard case review process for other exceptions to disclosure under FIPPA and PIPA, so that the Commissioner could continue to:

1. Ensure respect for the unique importance of solicitor-client privilege within the Canadian justice system generally and the exceptions to disclosure in FIPPA and PIPA;

2. Fulfill the Commissioner's mandate to investigate, inquire into and make orders concerning whether the exceptions to disclosure in s. 14 of FIPPA and s. 23(2)(a) of PIPA are properly claimed; and

3. Maintain an appropriate allocation of oversight resources between s. 14 of FIPPA and s. 23(2)(a) of PIPA and the other exceptions to the rights of access to information.

[139] This solicitor-client privilege case review process is a sound approach under the existing legislative framework. At the same time, the *Blood Tribe* decision has made it clear that both FIPPA and PIPA require more explicit language protecting the fundamentally important right of solicitor-client privilege and defining the Commissioner's independent review and adjudication mandate in this area. With respect to FIPPA, amendments are required to s. 44 to make it

clear that the Commissioner has the power to review records that a public body claims it is authorized to withhold on the basis of solicitor-client privilege. The need for express wording was confirmed in a recent decision of the Supreme Court of Newfoundland and Labrador where it was found that a statutory requirement on a public body to produce a record to the Commissioner was not sufficiently specific to capture documents subject to solicitor-client privilege.

[140] These amendments will protect the fundamentally important right of solicitor-client privilege while at the same time enabling the Commissioner to appropriately and effectively carry out the mandate that FIPPA imposes, as an act of legislative will, to verify claims of solicitor-client privilege.

Recommendation #19:

FIPPA should be amended by adding a new section that would explicitly permit the Commissioner to review records that are being withheld by a public body on the basis of solicitor-client privilege in order to verify that the privilege applies. The amendments should:

1. **Give the Commissioner specific, explicit authority to investigate, inquire into and issue orders concerning whether a public body or organization is authorized to refuse access to information or records on the ground of solicitor-client privilege under s. 14 of FIPPA; and**
2. **Expressly preserve and protect the substantive solicitor-client privilege despite the Commissioner's confidential examination of records in issue, when examination is necessary to verify the existence of the privilege.**
3. **The Commissioner's discretion to disclose information relating to the commission of an offence to the Attorney General pursuant to s. 47(4) of FIPPA should be removed.**

EXPLICIT POWERS TO RECEIVE STATISTICAL INFORMATION FROM PUBLIC BODIES

[141] Section 42 of FIPPA sets out the Commissioner's general powers to monitor how the Act is administered in order to ensure that its purposes are achieved. While the section gives the Commissioner the authority to conduct investigations and audits to ensure compliance with the Act, it does not provide the explicit authority to require public bodies to produce statistical and other information about their administration of freedom of information requests, including their compliance with timelines set out in the Act.

[142] There have been an increasing number of complaints from applicants about delays by some public bodies to respond to freedom of information requests. In 2006 there were 139 complaints received over time extensions and failure to comply with FIPPA. By 2009 the number of complaints received increased to 184.[37] Furthermore, the OIPC 2009 report entitled, *Timeliness of Government's Access to Information Responses*,[38] provides evidence that public bodies delay responding to requests from certain applicant groups.

[143] Pursuant to s. 63 of FIPPA, the head of the Ministry of Citizens' Services must submit an annual report with, among other things, statistics concerning the processing times of FOI reports. The OIPC 2009 Timeliness Report concludes that the Minister and ministry responsible for publishing annual statistics on FOI requests, the Ministry of Citizens' Services, does not fully comply with this requirement. Part of the Commissioner's duties is to monitor compliance with FIPPA, especially the completion of FOI requests in a timely fashion. In order to acquire the statistical and other pertinent information to analyze and monitor performance, the Commissioner needs the power to compel it. Therefore a change to s. 42, giving the Commissioner explicit power to compel public bodies to submit statistics and other information is required.

[144] We submitted this recommendation to the 2004 Special Committee, which approved of the idea and repeated the recommendation almost verbatim as recommendation #17. The current disposition of this recommendation by the government is "under consideration". The OIPC still strongly endorses this recommendation.

Recommendation #20:

Section 42 should be amended to explicitly give the Commissioner the power to require public bodies to submit statistical and other information related to their processing of freedom of information requests, in a form and manner that the Commissioner considers appropriate.

TIME LIMIT FOR STAY OF AN ORDER PENDING JUDICIAL REVIEW

[145] Section 59(2) of FIPPA requires a public body to comply with an order of the Commissioner within 30 days of delivery of the order. If an application for judicial review of the order is brought within 30 days, it imposes an automatic stay of the Commissioner's order unless the Court orders otherwise. Section 59(2) makes it unnecessary for a petitioner for judicial review to make an

[37] Statistics are from the Office of the Information and Privacy Commissioner Case Tracker.
[38] http://www.oipc.bc.ca/investigations/reports/F08-35580_Calendar_2008_Report_Card (Feb_2009). pdf.

interim motion to the Court for a stay of the Commissioner's order pending the disposition of the judicial review.

[146] There is currently no time limit on the length of a stay under FIPPA. A party can file an application for judicial review and then take no steps to pursue the application, leaving continuing uncertainty about the effect and timeliness of the Commissioner's order.

[147] The purpose of s. 59(2) is to give breathing space for a judicial review proceeding to be brought on for a hearing, not to promote delay or to frustrate rights under FIPPA. However, because the s. 59(2) automatic stay is not time-limited, a petitioner that neglects or refuses to proceed, expeditiously or at all, with the judicial review can easily abuse the stay. This is a problem with judicial reviews brought by third parties.

[148] Although judicial review is intended to be a summary process, a relatively simple judicial review of a Commissioner's order often engages, at the Supreme Court level alone, significant time (often one to two years) and expenses for participating parties, including the OIPC. For third-party initiated judicial reviews, the OIPC is often the only represented respondent.

[149] It is the OIPC's belief that an amendment to s. 59(2) should ensure that, after 60 days, if the applicant for judicial review has taken no further action, the Commissioner's order automatically comes into effect. The applicant would be permitted to appear in court within the 60 days and seek a further extension, with the Court possibly attaching conditions.

[150] The suggested amendments to s. 59(2) address delays and provide judicial oversight of the stay proceedings. The suggested timeline of 60 days and the discretion in the Court to vary or impose conditions is consistent with government policy as set out in s. 57 of the *Administrative Tribunals Act*.[39]

[151] The OIPC made a similar recommendation (number 30) on this matter to the 2004 Special Committee and the Committee agreed with the OIPC in making the recommendation that is set out below. Government's Disposition of Recommendations reports the status of this recommendation as "under consideration".

---

[39] **Section 57 of the Administrative Tribunals Act provides: Time limit for judicial review**
57(1) Unless this Act or the tribunal's enabling Act provides otherwise, an application for judicial review of a final decision of the tribunal must be commenced within 60 days of the date the decision is issued.
(2) Despite subsection (1), either before or after expiration of the time, the court may extend the time for making the application on terms the court considers proper, if it is satisfied that there are serious grounds for relief, there is a reasonable explanation for the delay and no substantial prejudice or hardship will result to a person affected by the delay.

Recommendation #21:

Section 59(2) should be amended and a new s. 59(3) added to inhibit abuse of the judicial review process by time-limiting the automatic stay of the Commissioner's order as follows:

(2) If an application for judicial review is brought before the end of the period referred to in subsection (1), the order of the Commissioner is stayed for 60 days from the date the application is brought.

(3) A court may abridge or extend, or impose conditions on, a stay of the order of the Commissioner under subsection (2).

ALLOW 90-DAY REVIEW TO BE EXTENDED

[152] Section 56(6) of FIPPA provides that an inquiry into a matter under review must be completed within 90 business days. Our experience in the past six years has been that it is not possible for the OIPC to complete reviews of all access requests within 90 days. To illustrate this point, the OIPC had to extend the time to complete 49% of the 586 request for review files that were closed in 2009.

[153] A recent decision of the Alberta Court of Appeal[40] highlighted the mandatory nature of that 90-day timeline in its interpretation of the analogous provision in the Alberta *Personal Information Protection Act*. It was held that the discretion of the Commissioner to extend that period under that Act must be exercised before the expiry of the 90-day period and on a case by case basis.

[154] Unfortunately, unlike the Alberta statute and most others in Canada, FIPPA is silent about the ability to extend the 90-day timeline. In British Columbia, s. 50(8) of PIPA allows the Commissioner to specify a later date. It reads as follows:

> 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.

[40] *Alberta Teachers' Association* v. *Alberta (Information and Privacy Commissioner)*, 2010 ABCA 26,

[155] FIPPA should be amended to make it consistent with PIPA and with other jurisdictions in Canada.

Recommendation #22:

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