IN THE MATTER OF THE ROYAL COMMISSION INTO FAMILY VIOLENCE

ATTACHMENT SW-39 TO STATEMENT OF SCOTT JAMES WIDMER

Date of document: 31 July 2015
Filed on behalf of: State of Victoria
Prepared by:
Victorian Government Solicitor's Office
Level 33
80 Collins Street
Melbourne VIC 3000

[redacted]

This is the attachment marked '**SW-39**' produced and shown to **SCOTT JAMES WIDMER** at the time of signing his Statement on 31 July 2015.

Before me: [redacted]

[redacted]
An Australian legal practitioner
within the meaning of the
Legal Profession Uniform Law (Victoria)

GOVERNMENT SUBMISSION

to the

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

March 15, 2010

Table of Contents

Executive Summary

Structure of Submission

This submission to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* (the FOIPP Act) consists of two general parts: part one provides a brief overview of FOIPP Act, its governance and administrative framework and a summary of amendments to the FOIPP Act; part two focuses on the protection of privacy providing an overview of the privacy provisions of the Act, the current operating environment for government, chapters focused on specific FOIPP Act issues experienced by ministries, the related challenges and how these can be addressed, and a conclusion section containing recommendations for amendments to the FOIPP Act.

Overview of the FOIPP Act

The FOIPP Act came into force on May 22, 1992 and was proclaimed in stages from 1992 through 1994, extending the Act to an expanded set of public bodies with each stage. The purpose of the FOIPP Act is two-fold: 1) to promote accountability by providing a right of access to records and information of public bodies; and 2) to protect personal information by prohibiting the unauthorized collection, use, disclosure, or storage of personal information by public bodies.

The FOIPP Act is prescriptive legislation, outlining in specific detail the rules and requirements respecting citizens' access to information rights and how to exercise them, and their right to privacy including what, when, why and how personal information can be collected, used, disclosed and retained by public bodies.

The FOIPP Act has been amended several times over the years, both in response to Special Committee reviews and in response to other reviews and developments. Some of the recent significant amendments to the Act include provisions to limit the storage and disclosure of personal information outside of Canada and allow disclosure for the purpose of an integrated or common program or activity. There are issues with the efficient and effective application of FOIPP Act, but amending the Act is controversial with stakeholders who perceive any change as a potential threat to the access and privacy rights enshrined in the legislation.

Governance and Administration of the FOIPP Act

The effective functioning and implementation of the FOIPP Act is dependent upon the ability, capacity and good faith actions of public bodies to carry out their duties and obligations under the Act. The responsible Minister, currently the Minister of Citizens' Services, is responsible for the administration of the Act and has certain regulatory authority. The Government's Chief Information Officer (GCIO), within the Ministry of Citizens' Services provides leadership, advice and support to ministries and manages the legislative change process. The Chief Executive Officer, Shared Services BC, through the Information Access Operations branch, is responsible for supporting ministries in meeting their operational records access and privacy needs. The Information and Privacy Commissioner, an independent Officer of the Legislature, has board

responsibility for overseeing and monitoring how the FOIPP Act is administered and for ensuring that its purposes are achieved.

Privacy Protection under the FOIPP Act

Privacy Rules and Requirements

The privacy provisions of the FOIPP Act are based on the principle that individuals own their personal information and that they have a general right to privacy. Part 3 of the Act prescribes detailed rules and requirements respecting the collection, use, disclosure, retention, security, accuracy and disposal of personal information by public bodies. This includes limitations on the collection, use and disclosure of personal information subject to certain allowable circumstances and exceptions; the right of an individual to review and correct their information; that personal information must be generally stored in Canada and rules respecting security, retention and disposal of personal information.

The Changing Environment

The world is a very different place than when the Act was first introduced 18 years ago. The use of computers, other technology, and the internet is now commonplace among British Columbians. Citizens are demanding convenient, accessible and on-time service, including from government. Government, in turn, is changing the way it does business and is increasingly looking to ways to enhance the quality of its services and its accessibility and responsiveness in meeting the needs of citizens through innovative program delivery and the use of new developments in information technology and management. This change in approach to service delivery includes an increasing move to horizontal and integrated program delivery models to more effectively serve citizens and achieve better outcomes for clients. The transformation of government service delivery is also a response to demographic pressures requiring government to deliver quality services with fewer staff by implementing innovative programs and leveraging information technology.

Addressing Barriers to Better Service Delivery

As highlighted in the Ministry chapters, ministries and government agencies face challenges in effectively sharing information to better meet the needs of clients, providing accessible and responsive services and promoting stronger engagement with citizens. British Columbia is not alone in addressing issues related to the effectiveness of information sharing to provide better services to citizens. Many jurisdictions, including commonwealth countries and European nations have recently initiated legislative amendment and policy reform processes to facilitate personal information flows designed to improve the effectiveness and efficiency of government services and service delivery to citizens.

Opportunities for Moving Forward

The B.C. Government is committed to enhancing services for British Columbians. Although B.C. is already delivering a wide range and scope of services to meet the needs of clients, improvements can be made to enhance the timeliness, accessibility, responsiveness and effectiveness of services. Government needs to leverage information sharing to produce better outcomes for citizens; provide services to citizens

in more efficient and effective and coordinated ways; and respond to client needs and service demands.

Recommendations for Change to Privacy Provisions of the FOIPP Act

Amendments to the FOIPP Act are needed to facilitate information sharing in order to support the B.C. government's ability to enhance services and implement new and innovative approaches to better meet the needs and expectations of citizens.

Following is summary of recommendations to amend the FOIPP Act to address the current challenges and to support government in providing more efficient, effective and responsive services to meet citizens' needs and expectations:

Consent, Collection and Disclosure	• Amend the consent provisions to allow an individual to consent to the collection, use or disclosure of their personal information by a public body (similar to the *Personal Information Protection Act* (PIPA)). • Amend the Act to allow for indirect collection by, and disclosure to and between all relevant public bodies, without consent, for purposes of integrated program or activity; where of benefit to the citizen and necessary to the delivery of the service or program; and/or for public health and safety. • Amend the Act to allow for indirect collection by, and disclosure to, non public bodies (RCMP, NGOs and social service providers, government and police agencies in other jurisdictions), without consent, for the purposes of integrated program or activity; where of benefit to the citizen and necessary to the delivery of the service or program and/or for public health and safety. • Amend the act to provide for implicit consent (similar to PIPA).
Consistent Purpose	• Amend the consistent purpose provisions to ensure the full, comprehensive and effective application of this provision as the basis for information sharing, including that consistent purpose covers information sharing (collection and disclosure) within the public body and between all public bodies where the sharing supports the provision of the program or service, and related services, to the citizen, meets the citizens' service needs and provide seamless, integrated program and service delivery (including integrated or common programs or activities addressing domestic violence, homelessness and integrated justice or crime reduction programs)
Common or Integrated Program or Activity	• Amend the Act to facilitate delivery of integrated programs by ensuring full and effective information sharing under common or integrated programs and activities (i.e., integrated or common programs or activities addressing domestic violence, homelessness and integrated justice or crime reduction programs) including: ○ recognizing the range and scope of potential common or integrated programs or activities to meet and serve the needs of citizens (not limited to programs or activities with structural arrangements, but rather based on delivery of a common or integrated function); ○ allowing for the collection and disclosure of personal

	information, both indirect and direct, within the common or integrated programs or activities among all relevant parties, including public bodies and non public bodies (RCMP, NGOs and social service providers, government and police agencies in other jurisdictions); and ○ streamlining and providing for the appropriate records management requirements to enable effective and efficient information sharing in a common or integrated program while ensuring the security and protection of personal information
Storage of Personal Information Outside of Canada	• Amend the provisions in the Act prohibiting the storage of information outside of Canada to take into account IT developments and advancements that make jurisdictional boundaries artificial, including social networking and other internet tools and mechanisms that can promote stronger citizen engagement and to take advantage of commercial and economic opportunities for storage and management of information including “cloud computing”.
Research and Evaluation	• Amend the Act to include language confirming a broader approach to research so that applied research into issues, facts, trends, etc. for the purpose of program planning and/or evaluation can be undertaken.
Other Recommendations	*Ministries of Attorney General and Public Safety and Solicitor General*: • Amend the Act to broaden the definition of “law enforcement” to include crime prevention or reduction programs and provide that information may be collected for these purposes; • Amend the Act to clearly recognize that the protection of custody setting security footage is integral to effective law enforcement and add an explicit reference in s. 15(1) that authorizes a public body to refuse to disclose information to an applicant that could reasonably harm the effectiveness of custody setting security systems; • Amend the Act to strengthen the protection of privacy of personal information in police audits and other oversight functions by exempting any records generated from *Police Act* audits and examinations from the access provisions of the Act; • Amend the Act to provide more appropriate timelines for compiling a major report for publication; • Amend the Act to change the term "record in a court file" to "court record" and include a current definition of "court record" that takes into account new technology such as “Court Services On-Line” that provides greater access by the public to court record information.
	Ministry of Housing and Social Development: • Change the definition of “personal information” to “private information” in recognition that not all personal information is private and sensitive (“private information” would include date of birth, government issued identification material, bank account numbers, credit card numbers, financial transaction information, biometric information, medical information, security related details, etc).

	Ministries of Health Services and Healthy Living and Sport • Adjust public body framework by amending the Act to recognize the changes to the "Health Sector" by defining "health care body" to reflect a "health sector family" model. Under this proposed model, the Ministry of Health Services would be the "parent" public body for the health sector with pre-eminent authority over the information necessary to manage the system; health authorities which play a subsidiary role in the management of the delivery of services in partnership with the ministry would form a "constellation" of bodies below the Ministry and these "child" bodies would take direction from the Ministry.
	Ministry of Citizens' Services: • Revise the collection provision to clearly state the point at which collection occurs.

Foreword

The government submission to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* (the FOIPP Act) consists of two general parts:

- **Part 1** provides a brief overview of the FOIPP Act, outlines the governance and administrative framework, and summarizes amendments to the Act;

- **Part 2** focuses on the protection of privacy framework in BC. It provides an overview of the privacy protection provisions under the FOIPP Act and the current environment in which government operates;

- **Part 3** is composed of chapters prepared by the ministries of: Attorney General and Public Safety and Solicitor General, Housing and Social Development, Children and Family Development, Health Services and Healthy Living and Sport, and Citizens' Services, outlining the challenges and issues faced by individual ministries with respect to the FOIPP Act; and a summary of the common themes and proposed recommendations for amending the FOIPP Act to ensure that government can better serve its citizens while maintaining protection of personal privacy.

PART 1 –
The *Freedom of Information and Protection of Privacy Act*

OVERVIEW OF THE FOIPP ACT

Passage and Implementation

The *Freedom of Information and Protection of Privacy Act* (FOIPP Act) was passed unanimously by the Legislature on May 22, 1992.

Implementation of the FOIPP Act was staged:

- in October 1993 the Act came into force for ministries, Crown corporations and other provincial agencies;
- in October 1994 the Act was extended to include local public bodies, including municipalities, municipal police boards, school boards, universities and colleges, hospitals and regional hospital boards; and
- in May 1995 self-governing professions including the College of Physicians and Surgeons, the Law Society of B.C., and the College of Teachers came under the purview of the Act.

Scope and Purposes of the FOIPP Act

The FOIPP Act applies to all records in the custody and control of public bodies. Public bodies include all ministries, crown corporations, provincial boards and councils, local government bodies and governing bodies of professions or occupations.

Balance of access to information and protection of privacy

The purposes of the FOIPP Act are to make public bodies more accountable to the public and to protect personal information by:

- providing the public a right of access to records held by public bodies;
- giving individuals a right of access to their own personal information, and the right to request a correction of this information;
- defining limited exceptions to the right of access;
- prohibiting the unauthorized collection, use and disclosure of personal information by public bodies; and
- providing for independent oversight and review of decisions made under the Act through the Information and Privacy Commissioner.

Prescriptive legislation

The FOIPP Act outlines in specific detail the rules and requirements for access and privacy; it was modeled on the prescriptive style of early Canadian privacy and access legislation, in particular the Ontario legislation. The FOIPP Act includes a distinct Part that prescribes detailed rules respecting citizen's access to information rights and how to exercise these including how to make a request, contents of the response, through to how access must be given. The second major part of the Act prescribes detailed

rules respecting what, when, why and how personal information can be collected, used, disclosed and retained by public bodies.

Amendments to the FOIPP Act

Section 80 of the FOIPP Act requires that the FOIPP Act be comprehensively reviewed every six years by a Special Committee of, and appointed by, the Legislative Assembly. A report containing recommendations on amendments to the FOIPP Act must be submitted to the Legislative Assembly within a year of the appointment of the committee. The current review is the third review undertaken[1].

The first Special Committee review, initiated in 1997 and completed in 1999, made a number of recommendations for amendment to the FOIPP Act (it had not been amended since 1993). In response to these recommendations the government launched a comprehensive two-phase review of the FOIPP Act with the objective "to increase openness in government and reduce compliance costs".

The first phase of this review was completed in April 2002 and resulted in a number of amendments to the FOIPP Act that were relatively limited in scope:

- responded to some of the recommendations of the Special Committee of the Legislative Assembly that reviewed the FOIPP Act from 1997-1999;
- addressed some immediate cost and compliance issues; and
- made some adjustments to the operations of the Office of the Information and Privacy Commissioner (OIPC) to assist that office in meeting its legislative responsibilities while meeting fiscal restraint targets.

The second phase involved an extensive review of the FOIPP Act as well as all suggestions for change made by ministries, stakeholders and the public. The resulting amendments were designed to:

- reduce regulation to comply with the deregulation initiative;
- improve access and privacy provisions;
- reduce compliance costs;
- address unintended consequences of the original wording of the FOIPP Act;
- position B.C. to lead Canadian jurisdictions in E-government initiatives; and,
- better realize the FOIPP Act's original intent.

The FOIPP Act has been amended seven times since 2002. Although some of the amendments have been relatively significant in terms of addressing specific matters, the goal of many amendments has been to address issues, such as those identified in the second phase of the FOIPP Act review, that relate to the administration and

[1] The first review commenced on October 4, 1997 and the Special Committee appointed to review the Act reported out on July 15, 1999; http://www.leg.bc.ca/cmt/36thParl/foi/1999/review_act.htm. The second review commenced on October 4, 2003, and the Committee reported in May 2004; http://www.leg.bc.ca/cmt/37thparl/session-5/foi/index.htm

application of the FOIPP Act to make it more functional given international trends and a changing operational environment.

Some of the most significant recent amendments have been to the privacy provisions of the FOIPP Act. These include amendments made in 2004, when British Columbia became the first, and only one of two governments in Canada, the other one being New Brunswick, to add provisions to the FOIPP Act to protect citizens from the application of the *USA Patriot Act* by limiting storage and disclosure of personal information outside of Canada. The amendments were prompted by the concerns of the B.C. Government Employee's Union and other stakeholders about Alternative Service Delivery outsourcing contracts being held outside of Canada, and the personal information of British Columbians potentially being subject to scrutiny under the *USA Patriot Act*. These provisions have resulted in an ongoing cascade of challenges and issues around the ability to take advantage of developments in information technology and information management. The 2004 amendments also prevented access to personal information from outside of Canada; added whistleblower protection for employees; and instituted fines for unauthorized disclosure of personal information.

In 2005, the FOIPP Act was amended to add a disclosure provision allowing for common or integrated programs or activities. Use of this provision to promote information sharing across ministries and government agencies providing a common service to a common group of clients has not been maximized given problems around the ability to also collect and use personal information in common or integrated programs or activities and share information with all partners in the common or integrated program or activity.

Despite the amendments that have been made issues regarding the efficient and effective application of the FOIPP Act by public bodies remain. Amending the FOIPP Act has been a controversial process with special interest groups often opposing any change to the FOIPP Act as a threat to the access and privacy rights inherent in the legislation.

Overall, the result of the various amendments, while aimed at improving the functionality and application of the FOIPP Act, have resulted in a complex, detailed and often misinterpreted set of privacy provisions. Given that the FOIPP Act imposes everyday requirements on government services and programs in terms of privacy assessment and protection practices, the complexity of the legislation is an issue for its effective implementation.

GOVERNANCE, MANAGEMENT AND ADMINISTRATION OF THE FOIPP ACT

The effective functioning and implementation of the FOIPP Act is dependent upon the ability, capacity and good faith actions of public bodies to carry out their duties and obligations under the FOIPP Act respecting the collection, use, disclosure, protection, retention and disposition of personal information.

The FOIPP Act establishes a minister with the responsibility for the administration of the FOIPP Act. Currently, the "minister responsible for the Act" is the Minister for

Citizens' Services. The Minister has regulation making power to amend the schedules to the FOIPP Act listing public bodies covered by the Act and is also responsible for certain operational functions generally related to exceptions under the Act. The Minister is responsible for preparing an annual report and publishing the personal information directory and may establish a consultative committee to make recommendations to the Minister about the operation of the FOIPP Act.

The GCIO, within the Ministry of Citizens' Services, provides leadership, support and services to ministries and other public bodies, to assist them in complying with their privacy and access obligations under the FOIPP Act. It also manages the legislative change process for the Province's privacy and access legislation and provides corporate privacy advice. The Information Access Operations (IAO), a branch of Shared Services BC, in the Ministry of Citizens' Services, provides operational support to ministries in fulfilling their obligations under the FOIPP Act.

The Information and Privacy Commissioner, an independent Officer of the Legislature, has broad responsibility for overseeing and monitoring how the FOIPP Act is administered and for ensuring that its purposes are achieved.

PART 2 – PROTECTION OF PRIVACY IN B.C.

OVERVIEW OF PRIVACY PROVISIONS

As noted, the FOIPP Act has a two-fold purpose: 1) to promote accountability by providing a right of access to records and information of public bodies; and 2) to protect personal information by prohibiting the unauthorized collection, use, disclosure, or storage of personal information by public bodies.

The FOIPP Act is based on the principle that individuals own their personal information and that they have a general right to privacy. This means that as a general practice public bodies should consider individuals as stakeholders in the collection, use and disclosure of personal information. Public bodies are expected to ensure the protection of personal information in their custody and control and must be prepared to inform individuals how their information is used and managed and be willing and able to address individuals' privacy concerns.

Personal Information

Under the FOIPP Act, "personal information" is recorded information about an identifiable individual. This includes an individual's name, address, blood type, educational history, employment history, financial information, birth date, eye colour, gender, race, and other such information. Personal information also includes seemingly innocuous separate items of information that when put together could allow someone to accurately infer information about an individual. The FOIPP Act specifically excludes business "contact information" from the definition of personal information. Contact information is information that enables an individual at a place of business to be contacted, and includes the individual's contact name, position name or title, business address, business phone number, business email, business fax number, and other such information.

Consistent with this right to privacy principle, Part 3 of the Act provides direction to public bodies regarding their responsibilities to protect the personal information they have in their custody or control and prescribes detailed rules and requirements respecting the collection, use, disclosure, retention, security, accuracy and disposal of personal information by public bodies:

Limitations on the Collection of Personal Information

- Public bodies may collect personal information only when it relates directly to and is necessary for operating a program or activity, for the purposes of law enforcement, or if authorized by an Act.

  Personal information about an individual must be collected directly from the individual the information is about. Exceptions to this direct collection requirement are:

  - where another method of collection is authorized by that individual, by the commissioner, by another Act;

- to provide for the medical treatment of the individual and it is not possible to collect the information directly;
- where disclosure to the public body is permitted for specific purposes; and
- for the purpose of determining suitability for an honour or award, for a court proceeding, for collecting a debt or fine or making a payment or law enforcement.

When collecting personal information directly from individuals, public bodies must inform the individual of the purpose of collecting the information, the legal authority for collecting it and provide the title, business address and business phone number of an officer or employee who can answer questions about the collection. If individuals object to the collection of their personal information, public bodies should be prepared to justify why it is necessary to collect it.

Access and Correction

- Individuals have a general right of access to their own personal information and the right to request correction of it. The ability of individuals to request access to and correct any factual inaccuracies with respect to their personal information enhances transparency and accountability and increases the accuracy of the information thus reducing the probability of any decisions being based on erroneous or incomplete information. Only factual information can be corrected; where the desired correction does not include a correction of factual information, and no correction is made to the record, the head of the public body must put a note on the file about the requested correction that was not made.

Limitations on the Use of Personal Information

- The use of personal information is also limited. Public bodies must ensure that personal information in their custody and control is used for the purpose for which it was collected, for a consistent purpose, or for a purpose for which information may be disclosed to a public body. An individual may also consent in writing to the use of their information.

Limitations on the Disclosure of Personal Information

- Public bodies must not disclose personal information under their custody and control except as authorized under the FOIPP Act. An employee, officer or director of a public body, or an employee or associate of a service provider, who knows that there has been an unauthorized disclosure of personal information must immediately notify the head of the public body.

- The FOIPP Act permits the disclosure of personal information under stipulated conditions, *which in some cases will differ depending on whether the disclosure is international or solely within Canada.* Some of the conditions authorizing the disclosure of personal information by a public body include: that the individual has consented to the disclosure; disclosure is authorized under an Act of the Province or Canada or under a treaty or agreement of the two governments; where the information is necessary for the performance of duties of the officials of the public body, or a service provider of the public body; to another public body if the disclosure is immediately necessary for the protection of health and safety of the officials of the public body; by a public body to an individual if compelling circumstances exist affecting a person's health or safety; for the purpose of collecting debts or money owing to the government of British Columbia or a public

body; and by a public body that is a law enforcement agency to another law enforcement agency in Canada or other country under a treaty or other similar arrangement. In making a decision to disclose personal information, a public body should balance the benefit of the disclosure with any potential harm resulting from the information's release.

- When a public body receives requests for personal information from other public bodies, private organizations, or elsewhere, *the onus is on the public body receiving the request to verify the authority for the disclosure.* For example, if the authority is an enactment, the receiving public body should require the requester to identify that authority by direct reference to the enactment. Sometimes a public body will receive a request from a foreign agency, court, state or another authority outside Canada for the disclosure of personal information that is not authorized by the FOIPP Act. In these circumstances, the public body is required to immediately notify the Minister responsible for the FOIPP Act (through the Ministry of Citizens' Services). The Minister may by order allow disclosure outside of Canada in specific cases or circumstances, subject to any restrictions the Minister considers advisable.

Storage and Access in Canada

- Personal information must be stored and accessed only in Canada, except if the individual consents to disclosure outside of Canada (in the manner prescribed by the FOIPP Act), or in other limited circumstances outlined by the FOIPP Act.

Retention of Personal Information

- Public bodies must retain personal information for one year if it is used to make a decision directly affecting the individual. Other legislative and policy requirements might also apply for the retention of personal information beyond what is required in the FOIPP Act (i.e., tax legislation might require a public body to retain financial records for a specified period, or a public body's records retention schedules might indicate that records are to be retained for a specific time for operational reasons). Maintaining personal information that is no longer required is a security liability. When all relevant retention requirements have been met and the personal information is no longer relevant for business or legal reasons, a public body should destroy the information in a manner that will not compromise the security or the privacy of the information.

Security of personal information held by public bodies

- Public bodies must make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure or disposal of personal information. Public bodies are required to ensure that personal information is protected by adequate physical, technical and procedural measures. While all personal information requires some degree of protection, the type of security measures taken should be consistent with the level of the sensitivity of the information (i.e., personal information related to an individual's health will be more sensitive and will require greater protection than a list of adult registrants for a swimming course).

Service Providers

- Personal information generated by a service provider under contract to a public body is likely subject to the requirements of the FOIPP Act. Under the FOIPP Act, a service provider is defined as a person retained under contract to perform services for a public body. Public bodies must take care to ensure that all service providers are aware of their responsibilities and obligations under the FOIPP Act. The

requirements of the FOIPP Act extend to employees and associates of the service provider who have access to or custody or control of personal information as a result of the service provider's contracts with the public body. By policy, for ministries, a Privacy Protection Schedule (PPS) must be attached to all contracts involving personal information. A PPS lays out the security, storage, use, retention, disclosure requirements and limitations required by the FOIPP Act, as well as a clause for termination for non-compliance. Any deviations from the standard PPS must be approved by the Ministry of Citizens' Services.

Role of Information and Privacy Commissioner

- The Information and Privacy Commissioner is responsible for conducting investigations and audits to ensure compliance with privacy requirements; informing the public about the FOIPP Act and receiving comments from the public about the administration of the FOIPP Act; investigating and attempting to resolve complaints that a duty imposed by FOIPP Act or the regulations has not been performed, or that personal information has been collected, used or disclosed in contravention of the FOIPP Act's privacy provisions; commenting on the implications for protection of privacy of proposed legislative schemes or programs of public bodies; and commenting on the implications for protection of privacy of automated systems for collection, storage, analysis or transfer of information and with respect to record linkage.

THE PRIVACY ENVIRONMENT – THEN AND NOW

Historical Context

When the FOIPP Act was amended in 1993 to increase the scope of the number of public bodies covered by the legislation, government announced that it was the finest legislation of its kind in North America and had the broadest scope of any similar legislation in Canada. [Hansard, July 21, 1993, Vol. 12, No. 13]

In terms of openness, the FOIPP Act covers the broadest range of public bodies, ensuring access by the public to information held by a wide range of government and public sector agencies. On the privacy side, it establishes a detailed framework for ensuring that personal information is only shared as authorized and under specific conditions and applies these requirements to that same broad range of government and public sector agencies.

However, much has changed since 1992 and the passage of the FOIPP Act. The world is a very different place - how government interacts with its citizens and provides services and, in turn, the expectations of citizens of government and government service delivery have changed significantly over the last 18 years. This has impacts for the way government uses and manages information as a resource and how well the FOIPP Act supports the new expectations of citizens.

External Environment

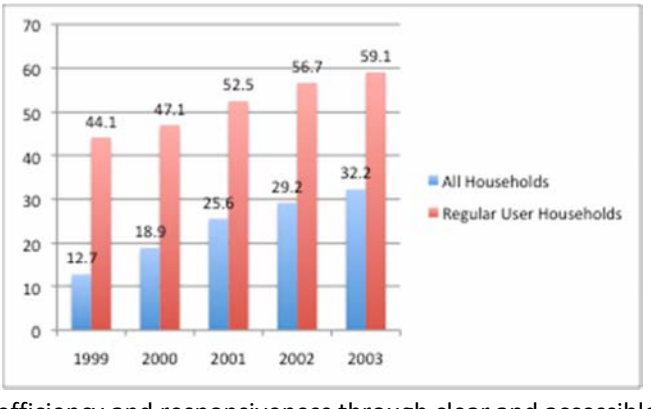
Technological developments, including the exponential growth in the use of personal computers and the introduction of the internet, has had a significant impact on citizens - how they work, shop, gather information, communicate with others, and manage their time.

In 2006, in Canada there were 87.6 computers per 100 people; second highest ranking in the world (Israel was 1st with 122.1 computers per 100 people and USA, 6th with 76.2 computers per 100 people).

[Source: Computer Ownership, Pocket World in Figures, The Economist, December 18, 2008 edition, economist.com http://www.economist.com/research/articlesBySubject/displayStory.cfm?story_id=12758865&subjectID=348909&fsrc=nwl]

Citizens today have become accustomed to high levels of service and convenience provided through commercial service providers. They expect responsive, timely and individualized services. Services are expected to meet individual needs and demands and be accessible through a range of different service channels. Many citizens want on line service, on their time and at their convenience.

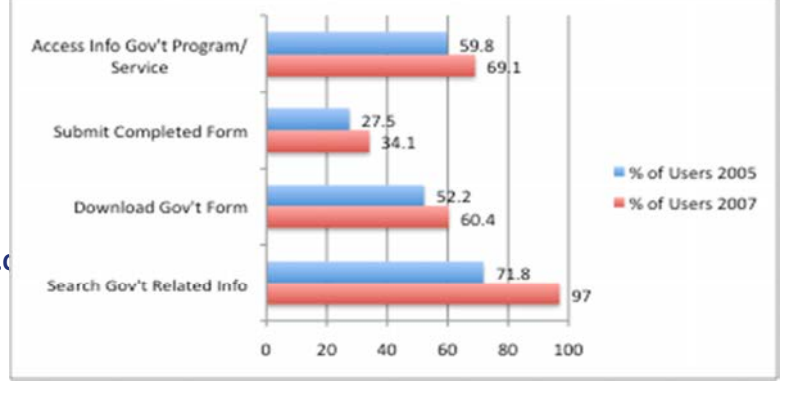
This includes services and programs provided by government. Historically, however, government agencies have often appeared confusing and bureaucratic to the citizens they serve, and it is not always apparent who can answer questions and resolve problems. Once the correct agency is contacted, the level of responsiveness may not match what customers have come to expect from commercial service providers.



% of Household Internet Use at Home - Accessing Government Information
[source: Stats Canada – following 2003 changed reporting format – see next graph]

Government is committed to enhancing its accessibility, efficiency and responsiveness through clear and accessible information and fast and convenient access to services. The goal is to be able to respond to citizens based on the individual citizen's needs and preferences and regardless of the method of communication, the nature of the request or the urgency of the request or need for service. From basic information requests to multi stage and agency case management, government is transforming its business to provide high quality citizen centred services.

% of Internet Users at Home who Searched for Information or Communicated with a Canadian Government On-Line



Leveraging current technological developments is key to meeting public expectations for service access and delivery and providing world-class citizen centric services, but this requires integrated and coordinated information sharing and information management. Elements of the FOIPP Act, including limitations on the collection, use and disclosure of information, the inability for an individual to consent to the collection of their information and the restriction on holding personal information outside of Canada are impediments and barriers to moving forward on various initiatives designed to meet citizens needs and demands and provide more accessible, efficient and effective range of services through different service models.

Furthermore, four out of five Canadian use social media, such as Facebook and Twitter, and almost 57 percent participate in social networks at least once a month (Forrester Research, 2009). The increasing use of social media tools presents a great opportunity for government to engage citizens and provide more direct and responsive services. Again, however, the prohibition of holding personal information outside of Canada, and other restrictions in the FOIPP Act are obstacles to taking advantage of this opportunity for enhancing engagement and better serving citizens.

Internal Government Environment

Eighteen years ago transactions between government and its citizens primarily took place by telephone, mail or through in person contacts. Information on citizens was generally held in paper files or in large databases. Services and programs were primarily delivered directly through ministries and government agencies. Government was organized into vertical structures with a single ministry or department responsible for delivering a particular program or service to a particular group of clients. There was a relatively limited need for sharing of specific personal information across programs and ministries and any information sharing was generally undertaken through in person contact or manual means (delivery or mailing of a document).

Government began to introduce personal computers into government workplaces in the early 1990s. Although it took several years to move to widespread use of personal computers across government, currently the vast majority of the government workforce has a personal computer.

Similar to the use of personal computers, the use of the internet was very limited until 1992. However, after the first commercial network came on stream in November 1992, its use expanded rapidly and the internet has become a broad and critical application for personal, household, business and government use.

Rise of the Internet

The design and development of the concept of the internet occurred throughout the 1970s, but it took a further 10 years to roll it out. Throughout the 1980s and into the early 1990s, the internet was funded by government and its use restricted to research, education and government. In 1992, the first independent commercial network came on stream. Delphi opened up an email connection in 1992 and offered full internet service by November 1992. The "world wide web" was invented in November, 1989, and its first image and text posted in 1992. By 1995, several commercial internet providers were in operation. The period of the late 1990s saw a period of exponential growth in the internet and World Wide Web and today it is widely used across all sectors – commercial, government and personal. The growth of wireless internet connectivity and growth in the use of small personal devices is the next big wave of development. Sites like Facebook, Twitter, Linked-In, YouTube, Flickr, Second Life, Delicious, blogs and wikis are extending the reach of the internet letting more people of all ages share information and their interests with others everywhere.

Today, the use of personal computers, the internet and the intranet, have become central to supporting the business of government. The development of information technology has substantially changed the nature of work for the public service workforce, including enhancing the ability of the workforce to communicate and share information internally, across programs and with their clients.

The way government organizes its services and does business has also changed substantially over the last several years. Much of this change can be credited to the growth in magnitude, scope and breadth of government services and the corresponding need to leverage technology and introduce other efficiency and effectiveness measures to meet service and program demands. Today, the B.C. Government is increasingly moving to a horizontal and integrated organizational structure to serve citizens in a more coordinated and effective way. Horizontal management – the coordination and management of a set of activities between two or more organizational units which serve a common group of clients and where the organizational units share overall goals or aims in serving those clients – results in better outcomes for citizens that cannot be achieved by units operating in isolation. Horizontal management is also more cost efficient and effective in terms of eliminating duplication and overlap.

An aging workforce is a demographic reality with significant impacts for the way government does business. In the future, government will need to deliver quality services with fewer people, which will demand higher levels of innovation than ever before. The BC Government is encouraging and promoting innovation on a project-by-project basis and working to build a culture of innovation across the organization. The use of new information technology is critical to the public service identifying and introducing better ways to do the work of the public service and meet the needs and expectations of British Columbians.

With this move to greater coordination and integration of services, to horizontal, rather than vertical and siloed program structures, government managers have become increasingly frustrated with the barriers in the FOIPP Act that prevent them from sharing information and taking advantage of the benefits of technology as this impacts their ability to implement innovative programs to benefit citizens.

Programs within individual ministries and agencies, multi-agency programs, and partners responsible for delivering common or integrated programs or activities, have become mired in differences of opinion as to what different aspects of the FOIPP Act means and allow in terms of information sharing. This impedes government's ability to move forward on delivering more effective and responsive services to citizens.

In 2007 and 2008, the GCIO, Ministry of Citizens' Services, undertook a major review of privacy and information sharing in government. The review was driven by the need to assess the current framework and environment for the sharing of information across government ministries and develop a strategy for enhancing information sharing to better serve clients and achieve better outcomes for citizens. Over the years several independent reports have called for greater information sharing between ministries and among ministries and other government bodies and agencies to reduce risk and provide more coordinated effective services to vulnerable populations. These include the Hughes Child and Youth Review, several reports of the Representative for Children and Youth, and the Keeping Women Safe Report on effective justice response to domestic violence.

The GCIO lead review found that the existing legislative, policy and practice environment is not conducive to information sharing. While some ministries are effectively sharing information internally and with other ministries, many other ministries, agencies and programs are not sharing to the extent needed to meet program and service needs. A key reason cited for this lack of information sharing is the FOIPP Act. The legislation is seen to be narrow, restrictive, unclear, and not supportive of information sharing even where that sharing of information can achieve strong benefit to citizens.

International Comparison

As noted earlier, the B.C. FOIPP Act is based on a prescriptive, rules based approach outlining in detail specific requirements and procedures to be followed by public bodies. Other jurisdictions, including European and commonwealth countries, have taken a more "principles based" approach to ensuring the protection of an individual's personal information.

Under a principles based approach, broad standards or principles for the protection of privacy are established and government agencies are expected to operate and act in a manner designed to achieve the intent of those principles. Australia has adopted a "hybrid" system based on broad privacy principles and some rules-based regulation in key areas. The benefits of a principles based approach include program specific methods to manage and protect personal information and better privacy protection overall given that programs are required to understand and address their own privacy requirements.

Some jurisdictions have recently initiated legislative amendment and policy reform processes to facilitate personal information flows designed to improve the effectiveness and efficiency of government services and service delivery to citizens.

The United Kingdom has initiated a broad information sharing strategy, and made recommendations for legislative change, with the goal of improving service delivery and reducing the duplication of efforts of several different public sector organizations collecting the same information, while ensuring high standards of privacy protection. Scotland has implemented *eCare*, a multi-agency information sharing framework that includes a central database repository of information to facilitate inter-agency integrated initiatives. High levels of privacy protection and security controls are part of the system, including organizational authorization and user level access requirements.

New Zealand's e-government plan includes objectives around enhancing government service capabilities by better connecting government to citizens and connecting various government agencies to each other to promote more accessible and coordinated services. Australia has also developed and released a broad information sharing strategy intended to break down barriers to information sharing in order to facilitate more effective information management in order to meet the needs of citizens. Addressing fragmented and inconsistent privacy legislation is recognized as a necessary step to achieving more effective information sharing and information management [2]

Governments internationally are addressing many of the same challenges and opportunities as British Columbia as they adjust their way of doing business and respond to technological change and demands and expectations of citizens. Effective information sharing is intrinsic to facilitating integrated programs and service delivery, providing more timely and accessible service to citizens, addressing the urgent and immediate needs of clients and supporting eGovernment initiatives that provide the foundation for efficient information sharing and management. Some jurisdictions are amending existing legislation or passing new legislation to facilitate information sharing, but within commonly accepted boundaries and within high standards of privacy practice. More effective and enhanced information sharing is also being supported in some jurisdictions by implementation of centralized information database systems and establishment of mandated government "centres of excellence".

CHALLENGES AND OPPORTUNITIES MOVING FORWARD

The B.C. Government is committed to enhancing services to British Columbians. While B.C. is currently delivering a wide range and scope of programs and services to meet the needs of citizens, improvements can be made to improve access to and responsiveness of services, achieve better outcomes through integrated programs and effective information sharing, and better meet citizens' demands for service delivery that are focused on individual demands, needs and circumstances.

[2] summarized from *Information Sharing Legislation and Strategies: A review of new international information management approaches*, Prepared by Knowledge Information Services, Office of the Government Chief Information Officer, December 2009.

The continued evolution and transformation of the way government delivers its services and programs has implications for how government uses information and technology to support innovative service delivery and to communicate with and engage citizens. Moving forward government needs to consider changes to the FOIPP Act to enable this change.

The challenges and issues, and proposed recommendations for changes to the FOIPP Act outlined in the Ministry submissions are organized around the following themes:

- ***Better Outcomes*** - Leveraging information sharing to produce better outcomes for citizens.

- ***Citizen Centred Service -*** Providing services to citizens more effectively and efficiently.

- ***Stronger Engagement -*** Responding to citizens' needs and service demands.

PART 3 – ISSUES & CHALLENGES FACED BY MINISTRIES

ATTORNEY GENERAL AND PUBLIC SAFETY AND SOLICITOR GENERAL

Ministry Mandate

Ministry of Attorney General

The Attorney General is the law officer for the Crown in British Columbia and has a legal duty to see that the administration of public affairs is in accordance with the law. The Ministry is responsible for legal services in two separate and distinct areas: the independent prosecution of criminal matters; and the provision of legal services to government. The Ministry provides civil legal services to Cabinet, ministries and certain public agencies to assist them in fulfilling their business objectives in accordance with the rule of law. The Ministry provides and funds justice services to support disputes to be settled out of court and manages the provincial funding of legal aid. The Ministry also provides court services, such as registry services and security, to British Columbia courts.

Ministry of Public Safety and Solicitor General

The Ministry of Public Safety and Solicitor General works to maintain and enhance public safety in every community across the province. The Ministry's responsibilities include: law enforcement and correctional services; crime prevention and restorative justice programs; prevention of human trafficking; victim services and addressing violence against women; protection programs; road safety; provincial emergency management and emergency social services; fire safety and prevention; consumer protection policy; and the BC Coroners Service.

Better Outcomes

Challenge #1: *Information Sharing – Collection and Disclosure among Sectors to Prevent the Risk of Domestic Violence*

Problem Description:

The safety of victims of domestic violence is jeopardized by the lack of clear authority within the FOIPP Act for the sharing of relevant victim, offender and case information among sectors. The police, Crown prosecutors, bail supervisors, child protection social workers, victim service providers, family justice counsellors, and others in the family justice, health and social systems, must be able to proactively share information in domestic violence cases to keep victims safe. The sharing of information about critical risk factors such as an offender's criminal record, history of violence, breaches of orders, and issues pertaining to a victim or potential victim's safety, are key aspects in risk and safety management for victims of domestic violence.

Several recent reports and initiatives have found that the lack of information sharing between sectors has had an adverse impact in domestic violence cases and have made recommendations to facilitate greater sharing of information:

- The 2006 report by the Honourable Ted Hughes titled *BC Children and Youth Review: An Independent Review of BC's Child Protection System* recommended amendments to allow public bodies to disclose personal information proactively in appropriate circumstances [page 119].
- In the 2009 report titled, *Honouring Christian Lee - No Private Matter: Protecting Children Living with Domestic Violence,* the Representative for Children and Youth wrote, that a coordinated and effective response to domestic violence should include, "information-sharing protocols and practices designed to ensure that all service providers and decision makers have the best possible information in a timely fashion" [page 54].
- Over the past 15 years, the B.C. Coroners Service has made recommendations in several domestic violence cases that police, government and community-based victim service agencies need to work together to enhance information sharing and coordinate risk management.
- The provincial Violence Against Women Steering Team has identified information sharing among health, social, and justice system partners as essential to both ensuring effective coordination in domestic violence cases and enhancing the safety of women and their children.
- In the 2008 report titled, *Keeping Women Safe: Eight Critical Components of an Effective Justice Response to Domestic Violence*, the cross sector project team lead by the Honourable Judge Josiah Wood recommended the following: "The Ministry of Labour and Citizens' Services, in consultation with the ministries of Attorney General and Public Safety and Solicitor General, should review FIPPA and propose amendments to enable justice system personnel to proactively share information with the victim and victim-serving agencies in domestic violence cases" [page 58].

Attempts to establish province-wide information sharing protocols in domestic violence cases have failed, in part, due to the uncertainty about the impact of privacy legislation on the ability to share information among various justice, social and health providers. In situations where it is unclear whether information can be shared without consent, a more cautious approach of non-disclosure is generally taken in terms of interpreting the collection and disclosure provisions under the FOIPP Act. This has led to situations where information in domestic violence cases is not routinely shared.

In order to conduct proper risk assessments and develop effective safety plans, information about critical risk factors must be shared in a consistent and timely manner. Lack of clear, routine information sharing can contribute to serious personal harm.

> ***Example*** *– A woman was shot five times after leaving her partner. Before the shooting, the woman had gone to police about her partner's other assaults against her and had let them know about his threats and access to weapons. Police requested and obtained a peace bond, but did not inform the woman that he*

> *already had a criminal record dating back several years for threats and violence committed against a former wife and members of her family. Police cited restrictions contained in privacy laws that made it difficult for them to release information about past criminal convictions. If this information had been shared with the victim or service providers working with her, it could have assisted in the development of a more effective safety plan.*

The need for sharing information to manage risk and safety is further highlighted in the 2009 report from the Representative for Children and Youth on the death of Christian Lee, a six year old boy who was killed alongside his mother and grandparents in Oak Bay by his father. In the report, it was noted that the Ministry of Children and Family Development and the police did not effectively exchange information in a timely manner and that information about the escalation of risk reported to police was not shared with other service providers. There were many professionals involved in the victims' lives and yet none had the benefit of all available information which is critical to managing risk and safety, including the child protection social worker who needed information regarding the dynamics of the parents' circumstances to properly assess the safety of Christian Lee [page 49].

FOIPP Act Challenges:

Collection and disclosure requirements under the FOIPP Act are unclear in terms of proactive cross sector information sharing, including in the case of domestic violence situations. While the FOIPP Act does allow disclosure without consent under certain circumstances, these exceptions need to be clarified, amended or new provisions passed to ensure the routine sharing of information between justice, social and health providers in domestic violence cases.

Disclosure without Consent: FOIPP Act Challenges

Under the FOIPP Act, consent is required before personal information can be disclosed to another agency or individual unless another provision within the FOIPP Act permits the disclosure without consent. Obtaining consent from the offender is not practical or appropriate in domestic violence cases as the process of obtaining consent from the offender may put the victim at higher risk of harm. Similarly, obtaining consent from the victim is neither practical nor prudent in domestic violence cases where it is likely that the victim and the offender will have ongoing contact.

While s. 33.1(1)(m) does allow the disclosure of information without consent if compelling circumstances exist that affect anyone's health or safety, this section is seen as imposing an excessively onerous test in situations where the timely sharing of relevant information amongst justice system partners and other service providers is critical to managing risk and safety. Preliminary interpretations received by the Ministry indicate that this provision is not intended for the routine release of information and requires a case-by-case analysis with significant deliberation before making a determination. However, the circumstances may not be recognized as compelling until after all available information is pooled and a clear picture emerges. In domestic violence cases a routine disclosure mechanism is required as justice, social and health providers must be able to easily share information where there are risk

concerns so that all parties can coordinate their actions in a timely fashion and have knowledge of changing circumstances in the case.

In addition to an onerous *test*, this section imposes an onerous *process* that is not appropriate in domestic violence cases. Section 33.1(1) (m) requires that the head of the public body (or delegate) must make a decision on whether to provide written notice of the disclosure to the individual the information is about. However, in domestic violence cases it would never be appropriate to mail notice of disclosure to the offender or the victim as this could compromise the safety of the victim.

The requirements of s. 33.1(1)(m) do not facilitate the regular and routine sharing of information amongst justice, social and health providers that is needed in domestic violence cases.

Indirect Collection: FOIPP Act Challenges

In addition to the challenges in relying on s. 33.1(1)(m) for the disclosure of information in domestic violence cases, the corresponding section in the FOIPP Act which allows for the indirect collection of information is also problematic. Section 27(1)(b) allows a public body to collect information indirectly from another public body if the information may be disclosed under ss. 33 – 36. For example, a family justice counsellor (Ministry of Attorney General) can collect information about offender risk factors (e.g. breaches and escalating violence) in a domestic violence case indirectly from an independent municipal police department if the disclosure is permitted under s. 33.1(1)(m). However, s. 27(1)(b) does not permit indirect collection of information from non-public bodies, such as the RCMP and non-government service providers. In the example described above, if it was the RCMP who had the information about the offender risk factors, the family justice counsellor would not be able to collect the information indirectly from the RCMP because the RCMP is a non-public body. In domestic violence cases, justice, social and health providers need to collect information indirectly from both public and non-public bodies in order to properly manage risk and safety.

Proposed Remedy:

- Amend the FOIPP Act to clarify the disclosure and collection of information among justice, social and health providers to protect the safety of victims in domestic violence cases.
- Collection: Amend s. 27(1)(b) to capture all sectors in domestic violence cases. Also, provide clarity for all sectors to collect information indirectly from each other on the victim and accused. Further, amend s. 27(1)(b) to clearly provide that the words “public body” applies to both the public body that the contracted service provider reports to and another public body such as Crown prosecutors, bail supervisors, police, social workers and health services.

  OR

- Collection: Amend s. 27(1)(c) by adding a new subsection (vi), such as: “enhancing a person’s safety or managing risk of harm in domestic violence cases”. This amendment would be applicable to service providers of public and non-public bodies.

- Disclosure: Similarly, amend s. 33.1(1) by adding a new subsection (q), suggest: "for the purposes of enhancing a person's safety or manage risk of harm in domestic violence cases".
- Note: Other amendments to the FOIPP Act may be needed following the development of the domestic violence initiative response to the recommendations from the Representative for Children and Youth and B.C. Coroners Service.

Benefit to Citizens:
Sharing information effectively is fundamental to coordinating services, preventing violence and promoting public and personal safety. In domestic violence cases, where police and various health, social and justice system partners each have information about a potentially dangerous situation, it is critical that information concerning the safety of victims be shared without barriers and used to protect those most vulnerable in our society.

The coordination of support services for victims of domestic violence is hindered by a lack of clarity on the collection and disclosure provisions under the FOIPP Act. The proper evaluation of risk and coordination of safety plans for victims of domestic violence cannot be achieved by justice personnel and service providers without enhanced information collection and disclosure provisions under the FOIPP Act. Effective assessment of offender risk and victim safety requires the sharing of information of both offenders and victims in a timely, consistent manner. By providing regular and routine collection and disclosure mechanisms to allow justice, social and health providers to share information in domestic violence cases, the FOIPP Act will enhance the response to domestic violence.

Challenge #2: *Common or Integrated Program or Activity - - Information Sharing by B.C. Corrections with Public Bodies and Private Organizations within Integrated Offender Management Programs*

Problem Description:
The Ministry of Public Safety and Solicitor General's Corrections Branch engages in integrated rehabilitative programs and offender management programs that involve work with other public bodies, non-government partner agencies (i.e. private contractors and non-profit agencies) and public bodies outside of B.C. Such programs are designed to provide coordinated support services to offenders, clients and victims in order to promote public safety and limit risks associated with re-offending.

The Downtown Vancouver Community Court and the Prolific Offender Management Project are examples of integrated programs. Each of these programs is designed to address the needs of offenders, clients and victims through integrated approaches. The programs involve B.C. ministries, health agencies, non-profit organizations, and federal government agencies. As a participant in these two integrated programs, the Corrections Branch supports the benefits that can be achieved through coordinated, multi-organization response to offender management. However, the Corrections Branch and other program partners have experienced several challenges during program establishment to ensure that information sharing within the programs comply with the FOIPP Act.

FOIPP Act Challenges:

Currently, under s. 26 of the FOIPP Act, a public body may only collect information that relates directly to one of its own operating programs or activities. Section 26 does not authorize collection of the same information by another body participating in the integrated program. Another issue is that under s. 27 of the FOIPP Act the information cannot be collected indirectly from a non-public body. The implication of this provision is that indirect collection is permitted from B.C. public bodies, but is not permitted from private service providers, non-profit organizations or federal public agencies (e.g. RCMP) that may be involved in program delivery.

In the rehabilitative context, individuals have multiple points of contact within the provincial government and with non-profit social service providers. However, the FOIPP Act does not currently recognize this or the fact that in order to manage rehabilitation programs, it is often necessary to engage non-government partner agencies and public bodies outside of B.C. This includes sharing information with federal justice partners and law enforcement agencies to support the delivery of integrated offender management programs.

British Columbia can achieve better outcomes for offender management if the statutory framework of the FOIPP Act is changed to permit the collection and disclosure of information among all parties within an integrated program. These parties include: public bodies (as defined currently in the FOIPP Act), law enforcement agencies, non-profit organizations, private service providers, or other government bodies inside or outside of B.C.

The main issue with s. 33.2(d) is that within such programs or activities disclosure is permitted under that section only to public body employees and not to other parties to the initiative. Unless the program meets another one of the disclosure provisions under ss. 33.1 or 33.2, the consent of participating offenders would have to be obtained before the disclosure could take place. In some situations, it is not practicable to obtain consent in a timely manner, and with this group of offenders, an absence of service and interventions on a timely basis may lead to poorer outcomes for the individual and physical or financial harm to the public.

Even where information sharing may be permitted under sections of the FOIPP Act other than those that deal specifically with integrated programs (s. 32.2(d)), the current structure of the Act is overly complex. Because the authority for sharing information with non-public bodies for the purposes of integrated programs is not explicitly referenced in the FOIPP Act, it may be necessary to engage in extensive analysis, often involving privacy advisors and legal counsel – all of which may delay the delivery of much needed social services.

Proposed Remedy:

For the purposes of better outcomes for integrated offender management:

- Collection: Amend ss. 26 and 27(1)(c) to allow for collection related to common or integrated programs beyond public bodies to all parties to the initiative including law enforcement agencies, non-profit organizations, private service providers, and other bodies inside or outside of B.C.

- Disclosure: Amend s. 33.2(d) to clarify that disclosure is permitted not only to public body employees, but to other parties necessary for the purposes of the integrated program.

Benefits to Citizens:
Evaluation results indicate that collaborative programs help support rehabilitative efforts and effective offender management. Integrated programs and cross -functional teams are increasingly becoming common methods of public service delivery. The ability to share information in a timely manner increases the effectiveness of programs designed to prevent individuals from re-offending and to assist them in obtaining necessary treatment, ultimately leading to increased public safety. It should be noted that the partner agencies referred to above are dedicated to helping the individual in question and /or ensuring public safety. Their employees are trained and specialize in achieving these objectives. Every day they work with individuals in difficult circumstances and must have all the relevant information to do their jobs effectively. The key is to revise our statutory framework to permit the transmission of relevant information so that their work can be undertaken in an efficient, seamless and timely manner.

Challenge #3: *Common or Integrated Program or Activity – Information Sharing within the Community Court, Prolific Offender Management Program and Justice Access Centres*

Problem Description:
In order to effectively deliver many of its services and to operate the justice system effectively, the Ministry of Attorney General must engage with agencies and sectors both within and outside the provincial government. The Ministry's justice system partners include the ministries of Public Safety and Solicitor General and Children and Family Development, as well as the RCMP and municipal police forces.

The Community Court, Prolific Offender Management Project, and Justice Access Centres, are all integrated approaches that are intended to respond more effectively to offenders and clients. They provide access to a variety of services beyond those provided by the Ministry alone, and even beyond other justice system partners to include social service providers. These services may need to collect and use information regarding addiction treatment, offender management or rehabilitation programs, physical and mental health, housing, victim services, or family counselling. In order to provide or refer clients to these services, it is often necessary to share information about clients and offenders who have multiple issues and needs that cannot be effectively addressed by a single justice system agency working in isolation. An integrated justice initiative with 10 partners would have to conduct an analysis of the collection, use, and disclosure of each possible piece of personal information that might be shared between each of the 10 agencies. Such a matrix would have thousands of cells and would not be helpful in guiding staff. Nonetheless, this is what would normally be expected and required under the Act.

Example: Downtown Community Court *- "Robert Wagner" suffers from addiction and likely a mental health illness that has not been diagnosed. Robert lives in Vancouver's downtown and has had no work for over two years. Robert has come in contact with the justice system on several prior occasions. At this time, Robert has been arrested and is facing several charges including possession of stolen property and possession of prohibited substances under the* Controlled Drugs and Substances Act*.*

While in the community court cells, Robert receives duty counsel services and is advised that information necessary to put together an effective solution to his problems may be shared among agencies in the community court. Justice, health and social service agencies share information that is in their possession and help Crown counsel and defense counsel formulate their positions for court that speak to Robert's circumstances and possible services and help. Robert is sentenced in the community court and the sentence considers the opportunities identified by the professionals to effectively manage his criminal behaviour in the community.

After court, Robert meets with his case worker in the community court and other service professionals, and, with Robert's input, the case worker and other professionals develop a coordinated long term plan with the view to address the issues that are underlying Robert's criminal behaviour. Robert's housing situation is assessed and a more appropriate residence found. An addiction treatment placement accessible to Robert by public transit is being sought. Robert is working directly with a mental health professional and is now receiving appropriate medication. Robert's financial situation has also improved as he now receives disability assistance and the cheques are directed to his new residence. Robert continues meeting with his case manager and his progress is reviewed with the integrated team of professionals in the community court; the plan is adjusted as necessary. This integrated approach ensures that agencies are not working at cross-purposes and are better able to support Robert to make changes in his life.

Example: Prolific Offender Management - *"Joe Smith" has been one of the most chronic offenders in his community. He has 70 prior convictions, mostly for property crimes and assaults and has a serious substance abuse problem. He has been in and out of jail for 15 years, since he was 20 years old. Joe has been an ongoing threat to community safety and uses a great deal of resources from different government services. After being notified that he was identified as a prolific offender and that he must make a change, but that he will be supported in doing so, he indicates a readiness to try. Police have spoken with him and bring his case to the Prolific Offender Management team, arguing that the offender is ready to stop offending and overcome his drug addiction due to a number of positive circumstances in his life, including a more stable home life and a child.*

A number of members of the team put together a plan with the offender – his probation officer, alcohol and drug counsellor, a recovery society director, and Crown Counsel. Police work with a local treatment facility to arrange treatment. The Ministry of Housing and Social Development, probation, and addiction counsellors support the offender in moving to get away from the associates who

have had a significant negative impact on him. The team also supports a lenient approach by Crown counsel to minor relapses.

Only a coordinated effort through an integrated program like the Prolific Offender Management Pilot program creates a realistic opportunity for Joe to stop offending. Without permission to share information, this kind of intervention could not occur and Joe would continue to be a chronic threat to his community.

FOIPP Act Challenges:

The current structure of the FOIPP Act is overly complex and difficult to understand, and requires staff to try to slot their work into an often confusing set of categories. Staff who attempt to apply the Act to their programs often become bogged down in extensive analysis, paperwork, negotiation, and administration. Privacy advisors have emerged in every sector to provide advice and interpretation, but interpretation and approaches vary significantly from one person and from one agency to the next. There remain a number of important privacy-related provisions in the Act that have not yet been adjudicated by the Information and Privacy Commissioner, leaving staff and legal counsel without authoritative guidance beyond the statutory language itself.

The challenges with applying the collection, use and disclosure provisions of the FOIPP Act were particularly evident in setting up information sharing frameworks for the two justice reform projects described above: the Prolific Offender Management Pilot Project and the Downtown Vancouver Community Court. For both these projects, information sharing is of significant benefit to the accused, for reduction of their criminal behaviour, and for the protection of the public.

Over a year and a half, each of these projects took hundreds of hours of staff time, analysis, and creation of numerous documents such as information sharing protocols, matrices of rationale for collection use and disclosure, privacy impact assessment, training materials, letters to individual team members, and a Memorandum of Understanding (MOU).

Lack of policy specific to information sharing for the purposes of integrated programs such as the Prolific Offender Management Pilot Project or the Downtown Community Court leaves the agencies involved with no guidance on how to correctly interpret the meaning of the Act in this context and specifically s. 33.2 of the FOIPP Act. As a result, agencies seek direction from the Office of the Chief Information Office on a program by program basis through the privacy impact assessment process. This approach is extremely time consuming as it requires Office of the Chief Information Office staff to learn and understand each program in great detail and ministries to assist in this process. It also leaves ministries without certainty as to how to structure the program and, once the investment is made, whether it would be appropriate for the program to continue in the original format until the privacy impact assessment is signed off.

Health authorities are important partners in integrated justice, health and social services programs. Currently, sharing of information within integrated programs is guided by each authority's interpretation of the legislation. Only through information sharing protocols or MOUs with ministries, on a program by program basis, are policy

and operational procedures for integrated programs developed. This is again a long and onerous process and the outcome is largely a negotiated solution that is challenged to satisfy all partners on all points. As it is important to err on the side of non disclosure, in the absence of specific rules to guide the parties, opportunities for integrated service delivery solutions are often not pursued.

It is not feasible to spend years developing an information sharing policy for each new project that may still result in staff feeling uncertain whether they have complied with the Act. Staff need 'permission' to do their jobs and to make decisions as professionals. In order to support them, a statutory environment is needed that provides clear direction on when and how information can be shared.

Information sharing among the various justice system partners is critical to providing timely and effective justice services. There are a number of ways in which the current statutory and policy environment for information and privacy impedes information sharing among partners.

First, the FOIPP Act is very complex and it is often difficult for line staff to understand the duties and obligations it imposes on them, particularly when developing new approaches to public safety. In addition, a number of significant privacy provisions of the Act have not yet been adjudicated and fleshed out in decisions from the OIPC, which means that, more than fifteen years after the Act came into force, staff are still in many cases operating with only the statutory language to guide them. Contravening some of the Act's privacy provisions constitute offences – for example, unauthorized disclosure of personal information is an offence, but unauthorized collection is not – and staff are understandably fearful of doing so but are often unsure about what they can and can't do. The development of new programs and approaches is often delayed by extensive analysis, consultation and legal advice on potential privacy implications, reducing the ability of the Ministry of Attorney General and its justice partners to respond promptly to trends in the justice system.

The structure of the FOIPP Act divides the tests for collection, use and disclosure of personal information. Since information sharing involves one person or agency disclosing information and another collecting it, both parts of the Act need to be satisfied. However, the Act's rules about collection are more stringent than those about disclosure and thus even in an integrated program, it may happen that one party can disclose the information, but the other cannot collect and use it to provide the required services. In particular, there is no clear authority for information sharing between "public bodies" as defined in the Act and those agencies that are not "public bodies" (such as the RCMP and non-government service providers). Government may sometimes rely on the "consistent purpose" provisions in the Act, but the meaning of these provisions has still been largely untested in reviews before the Commissioner.

The following illustrates some of the difficulties with the FOIPP Act:

- Section 26 prohibits collection of information that is not strictly necessary for the particular public body even though, once collected, it could perhaps be disclosed under s. 33.2. The two sections do not work together and are confusing for staff to work through.

- Indirect information collection (that is, information collected from another body rather than directly from the individual) must be authorized by s. 27 of the Act. That section allows indirect collection from another public body but not from a non-public body, so collecting from another Ministry is allowed, but not from the RCMP or a non-governmental agency.
- While collection and disclosure of personal information are permitted for law enforcement purposes, the definition of "law enforcement" does not reflect the true extent of that work today. Law enforcement involves more than specific investigations by police or court proceedings that are reactive in nature because they occur in response to a crime that has been committed. It necessarily involves the collaborative work of justice system, health and social services professionals to actively address crime prevention and crime reduction.

Proposed Remedy:

Broaden the definition of "law enforcement":

A number of the FOIPP Act's sections include exceptions for information collection, use and disclosure for the purpose of law enforcement. The Ministry proposes an amendment to broaden the definition of "law enforcement" to include integrated justice programs that actively seek to reduce crime, e.g. by managing offenders, or through crime reduction or crime prevention initiatives.

Amendments specific to integrated justice programs:

- Amend ss. 26 and 27(1)(c) to allow for information collection by integrated justice programs; and
- Amend s. 34 to clarify that a consistent purpose includes all agencies participating in an integrated justice program.

Information-sharing rules based on function:

Rules respecting collection, use and disclosure of information for integrated justice programs should be developed on a functional basis rather than a "public body" vs. "non-public body" basis. That is, the FOIPP Act should recognize that multiple partners who are part of a bona fide ongoing integrated program should be able to share personal information for the purposes for which the program is intended.

- Amend ss. 26 and 27 to allow for information collection by integrated justice programs;
- Amend s. 33.2(d) to clarify that disclosure is permitted not only to public body employees but to other parties necessary for the purposes of the integrated program; and
- Amend s. 33.1(c) to authorize disclosure to public bodies in other provinces or territories.

Benefit to Citizens:

Information sharing among justice and social service partners to increase public safety is good public policy, is critical for an effective justice system, and to avoid gaps or overlaps in services. The Ministry and the justice system as a whole operate within

resource constraints. The Ministry works hard to develop innovative and effective approaches to reduce crime and enhance public safety. The public rightly expects that the Ministry will collaborate with its justice system partners and other social service agencies to provide British Columbians with an effective and efficient justice system.

Sharing information effectively is fundamental to coordinating services effectively, preventing violence and promoting public safety. Justice system clients benefit from effectively run integrated programs as their multiple needs are attended to on a more timely basis. Better management of offenders and other system participants enhances public safety and improves public confidence in the justice system.

The proposed amendments would support effective service delivery by the Ministry and its partner agencies, including Health Services, Housing and Social Development, independent municipal police, RCMP, courts, Forensic Psychiatric Services, and Youth Justice. The amendments would enhance public safety by creating a statutory framework that supports:

- Integrated outreach and offender management programs to address the root causes of crime including mental illness, addictions and homelessness;
- Integrated teams of enforcement and social service agencies to reduce risk and support behaviour change in addicted and mentally ill offenders;
- Improved information and risk management processes to support bail decisions; and,
- Closer monitoring and intensive intervention with high-risk offenders.

The clear trend in the justice system is for collaboration and co-operation amongst a variety of provincial, federal, local and non-government agencies to address the multiple needs of justice system participants. Increasingly, public safety depends upon the ability of agencies and organizations to share information. By facilitating information sharing for the purposes of administering integrated programs, the Ministry's proposed remedies will help to enhance public safety, prevent violence and aid victims.

Challenge #4: *Protection of Privacy - Acknowledge that B.C. Corrections' Security Systems Including Video Surveillance are Integral to Law Enforcement*

Problem Description:

The Ministry of Public Safety and Solicitor General recognizes that the corrections environment is increasingly complex as the justice system is encountering more violent and prolific offenders affiliated to organized crime. The changing profile of offenders means that victims in the community face greater risks to health and safety. In the context of increasingly sophisticated offenders, the security of correctional facilities requires that the details of security systems remain guarded. The disclosure of any B.C. Corrections video surveillance footage may reveal deficits within the holistic surveillance system and negatively affect correctional centers and public safety.

Example - *John Doe recently released to the community, requests Digital Video Recording of a one-hour period during which he was exercising in the yard. After review and consideration of relevant FOIPP Act exceptions to disclosure, the recording is released by B.C. Corrections in its entirety as no supporting section is found to withhold this information. John Doe then studies the recording to determine blind spots and the location of any adjacent cameras. With this information, he counsels a friend still incarcerated, on how to avert security for the best location to stage an assault on a fellow inmate.*

Or, based on the example above, Mr. Doe determines that "blind spots" exist around the perimeter of the correctional centre. With this information, he determines where drugs and other contraband can be surreptitiously dropped in the centre. The correctional centre is surrounded by residential properties that experience an increase in trespassing and property crime due to an influx of drug trafficking. In addition, the increased availability of contraband within the centre decreases the effectiveness of rehabilitative measures and negatively impacts reintegration to the community.

FOIPP Act Challenges:

Section 15(1) of FIPPA does not currently acknowledge that B.C. Corrections' security systems, such as video surveillance, are integral to law enforcement. Section 15(1) (l) provides only that the head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to harm the security of any property or system, including a building, a vehicle, a computer system or a communications system. Not including B.C. Corrections' security systems under the law enforcement exception continues to leave the security systems exposed, leading to the potential for escapes and violence both in correctional centers and the community.

Although there are indications that the Corrections Branch may correctly use the FOIPP Act provision under s. 15(1)(l) to protect the security of a property such as a corrections facility or a surveillance "system", it is not clear in every situation. The Corrections Branch is currently in a mediation process with OIPC with respect to public disclosure of security material, specifically Digital Video Recording and the use of ss. 15 and 22 of the FOIPP Act to protect public access to sensitive security footage.

Considerable resources have been invested by, the Corrections Branch, the applicant, and the OIPC. The applicant first made a request for access to video recordings in April 2006, which was subsequently considered by an OIPC adjudicator. The OIPC adjudicator issued an order requiring the release of some of the security footage in June 2008 that was challenged by the Corrections Branch through a judicial review. The matter was left undecided at the judicial review stage and returned to the OIPC for additional analysis. In total, almost four years have passed since the initial request for access without further clarity on the ability to prevent access to custody centre security footage under s. 15 of the FOIPP Act.

Although s. 22 of the FOIPP Act may apply in cases where it's possible to establish the identity of third party individuals, it may not always be the case that custody centre video recordings contain third party images. Section 19 of the FOIPP Act may also apply

in cases where the release of a specific video recording may put a particular person at risk. However, it is not the case that s. 19 can be applied to protect custody centre security footage from public release in cases where individuals may be looking to exploit gaps in security coverage or quality for the purpose of criminal and/or harmful motives.

Proposed Remedy:

- Disclosure: Clearly establish that the protection of custody setting security footage is integral to effective law enforcement under s. 15(1) of the FOIPP Act. Add an explicit reference to s. 15(1) that authorizes a public body to refuse to disclose information to an applicant that could reasonably harm the effectiveness of custody setting security systems.

Benefit to Citizens:

Amending s. 15(1) to include B.C. Corrections' security systems would support efforts to maintain the safety of inmates and staff, reduce opportunities for the delivery of contraband to correctional centers, and enhance public safety.

Citizen Centred Service

Challenge #5: *Consent – Police Disclosure of Victims' Personal Information to Victim Service Providers After a Crime has Occurred*

Problem Description:

Police-based victim service programs are delivered on contract with the Ministry of Public Safety and Solicitor General and operate out of independent municipal police departments and RCMP detachments. Victims Services[3] offers critical incident response, criminal justice information, practical and emotional support, safety planning, and referral services to victims of crime.

Conflicting interpretations regarding the collection and disclosure of information under the FOIPP Act have been a barrier to victims receiving these essential support services.

FOIPP Act Challenges:

The current practice, which is based upon direction from the provincial and federal privacy commissioners, is a consent based model. Police attempt to obtain consent from victims before disclosing their information to police-based victim services.

Issues with consent-based model

There are significant challenges with relying on the police to obtain consent from a victim who is in a state of crisis or trauma. After a violent crime, the victim may be fearful, humiliated, distraught, confused, in shock, physically injured or under the

[3] The Ministry funds two main types of victim service programs: police-based and community-based victim services. This issue is focused on police-based victim service programs. The Ministry has protocols in place to govern the referral of victims of family and sexual violence from police-based to community-based victim service programs. Independent municipal police are subject to the *Freedom of Information and Protection of Privacy Act.* The RCMP is subject to the *Privacy Act* (Canada).

influence of drugs or alcohol. They may not be able to understand, process, or respond to the request for consent. Requiring explicit consent in order to facilitate basic essential service delivery is not responsive to the needs of the victim. The Privacy Commissioner of Canada has acknowledged that a victim in the immediate aftermath of an incident may not be in a state of mind to either receive information or provide consent.

In addition, the Federal Ombudsman for Victims of Crime points out that, at the scene of the crime, victims will not understand or retain information given to them. Victims may require information to be repeated several times. Simply handing a pamphlet about victim services to a person in trauma is not adequate. The Ombudsman also notes that "despite all the progress that has been made to develop a wide variety of victim services at all stages in the criminal justice process, victims are not aware of the services available or understand how these services may help them. This remains a major barrier to assisting victims." [4]

A multi-site survey of victims of crime and justice professionals in Canada found that many victims wanted victim services to initiate contact with them directly. In the survey many victims noted that they "are often too traumatized or embarrassed to call, therefore, may not receive help unless victim services contact them."[5]

Research with women who were victims of violence within relationships revealed that when a victim reports an incident they are looking for protection, information, validation, and respect. The 2003 National Victims of Crime Conference revealed:

> Victims felt empowered when the various agencies - from police to Crown attorneys, to the judiciary to victim services-functioned as an integrated team. Women particularly felt re-victimized when they had to re-tell their stories to each person they came in contact with during the process. Most women wanted agencies to act proactively and share their information with other agencies.[6]

If police are not able to obtain consent at the crime scene, the victim will not receive victim services at the crucial time, and the impacts of the crime may be further exacerbated. It is essential that victims receive victim services in a timely and effective manner. Victims need immediate practical support, emotional support and safety planning which are provided by victim service workers. They also need to be advised in a timely manner of benefits that may be available, in particular, benefits through the Crime Victim Assistance Program has a deadline for application of one year from the date of the crime, with the exception of sexual offences.

---

[4] Steve Sullivan, Federal Victim Ombudsman. Letter to the Honourable Peter Van Loan, Minister of Public Safety; RCMP *Referrals to Victim Services* (October 23, 2009).

[5] Department of Justice Canada, *Multi-Site Survey of Victims of Crime and Criminal Justice Professionals across Canada* (2004) p. 36.

[6] Department of Justice Canada, *2003 National Victims of Crime Conference* (November 3-5, 2003) (www.canada.justice.gc.ca/en/ps/voc/publications/nvc/NVCen.pdf) p. 24.

It is particularly essential for victims of domestic violence to receive immediate victim services. These victims have a relationship with the offender, and the likelihood of repeat offences is high. If the victim does not receive victim services, she or he may not receive crucial safety planning assistance or relevant benefits and services, such as protective measures and counselling through the Crime Victim Assistance Program.

Rather than relying on police to obtain written consent, the better practice is to enable victim service workers to contact victims of crime directly with or without the prior consent of the victim. Police-based victim service programs are integrated into the operations of police departments throughout B.C. and operationally supervised by the police. Police-based victim service workers in B.C receive training from the Ministry, Police Victim Services Association of B.C., and from the departments or detachments where they work. Security standards for all police-based victim service programs operating in independent municipal police departments require that all employees hold level 3 security clearances and sign an oath of confidentiality. Also, additional screening and advanced training is required for designated employees for access to police file information and the Police Records Information Management Environment system.

Disclosure without consent – lack of clarity on FOIPP Act interpretations

There are currently provisions under s. 33 of the FOIPP Act for public bodies to disclose information without consent, including "consistent use", "common or integrated program" and "compelling circumstances". However, there is a lack of clarity on these subsections. The Ministry has had interpretations and analysis that provide differing views on which provisions may be relied upon to allow for the sharing of information without consent.

In order to ensure that victims of crime receive the services they need in the aftermath of crime, clear authority is required to enable police to routinely share essential information with victim services to facilitate timely and effective service delivery.

"Necessary Information" – lack of clarity on FOIPP Act interpretations

There are also differing views on what information is "necessary" for victim services to collect in order to perform their duties. The following information is required to inform a victim service worker of the proper supports, services, safety planning strategies and referrals that may be required to effectively assist a victim and provide services in accordance with the *Victim of Crimes Act*:

- the victim's name and contact information or if the victim is deceased, their next of kin's name and contact information;
- a brief synopsis of the incident (to avoid asking the victim directly, which will lead to victim discussing "evidence");
- the relationship of the accused to the victim (the likelihood of repeat offences is directly related to the relationship between the victim and accused, so is necessary for the safety of both the victim and the worker);
- special circumstances such as language requirements or cultural concerns;
- the release conditions of the accused, such as no-contact orders or bail conditions (directly related to the safety of both the victim and the worker);
- the victim's safety concerns; and

- the case status, such as whether or not the suspect/accused is known, has been arrested or is in custody.

Indirect Collection of Personal Information by Victim Service Programs

In addition to the need for clear authority for police to routinely disclose personal information to victim service programs without consent, there must also be clear authority for victim service programs to indirectly collect this information from police agencies. There are differing views regarding the ability of victim service programs, as service providers, to collect information indirectly from police under s. 27(1)(b) of the FOIPP Act.

Proposed Remedy:

- Collection: Amend s. 27(1)(c) to allow public bodies to collect information indirectly for the purposes of delivering victim services by adding a new subsection (v), suggest: "delivering victim services in partnership with a law enforcement agency".
- Disclosure: Amend s. 33.1(2) to allow a law enforcement agency to disclose personal information to a victim service provider by adding a new subsection (c), suggest: "to a victim service provider operating in partnership with a law enforcement agency for the purposes of delivering victim services".

Benefits to Citizens:

A Canadian societal value is to protect those most vulnerable in our society. The need for a crime victim's prior written consent to disclose their personal information cannot trump their personal safety or the opportunity to engage with trained victim service workers to deal with trauma and receive emotional and practical support in a time of great need. In order for victims to access victim services, they first need to be informed about victim services.

Victim services play a significant role in helping victims with risk identification, safety planning and successful participation in the criminal justice process. Enhancing the collection and disclosure provisions under the FOIPP Act is essential to ensure that victims of crime in B.C. have timely access to victim services to enhance their safety and reduce the impact of crime and trauma.

Further, amendments to collection and disclosure provisions will assist in meeting the goals of the *Victims of Crime Act* to promote equal access to victim services, have victims adequately protected against intimidation and retaliation, and to give proper recognition to the victim's need for timely investigation and prosecution of offences. The risks associated with not providing the relevant and necessary information that is required for the provision of victim services can be significant as early intervention and support is often critical to victims' safety and well-being.

Stronger Engagement

Challenge #6: *Protection of Privacy - Strengthening Protection of Privacy of Personal Information in Police Audits and Other Police Oversight Functions*

Problem Description:

In the Ministry of Public Safety and Solicitor General, the functions of the Director of Police Services under ss. 40, 42, 43 and 44 of the *Police Act* (inspections, evaluations, studies, inquiries and investigations) are critical to policing oversight, policing accountability, and enhancing the effectiveness of policing services. Policing services are delivered by municipal police detachments that are governed by independent police boards. The Ministry's Police Services Division (PSD) must have the ability to independently collect information and data from departments and key individuals in order to succeed in fulfilling its functions under the *Police Act*. Reports and recommendations from police audits are public information.

In conducting *Police Act* audits of police departments a primary data collection process is interviewing and/or surveying members of the department. Even though the audit team informs the interviewee that they will not be named or identified by rank or position, the audit team is unable to guarantee absolute confidentiality given that PSD's audit records are subject to freedom of information provisions under the FOIPP Act. One consequence, for example, is that during past audits of departments, some officers have refused to disclose on the record sensitive information about incidents of harassment by colleagues or supervisors.

Further, during the course of an audit a number of non-police persons may be interviewed, such as community victim service groups, local Crown and civilian members. The FOIPP Act issue is one of ensuring that all interviewees are confident that they can speak frankly and reveal information that they may not otherwise divulge. Vetting of personal identifiers from audit records may not always remove the possibility that a person can be identified given the context of the department's environment or a specific incident.

Records arising out of or related to evaluating programs or studies require an explicit exemption to disclosure under the FOIPP Act in order to better protect personal information. Guarantees of confidentiality would better foster an environment of willingness among police departments, police officers, and citizens to participate openly and candidly in audits and examinations of policing. PSD's inability to guarantee confidentiality fosters uncertainty and unwillingness among officers and citizens to provide information. If PSD cannot obtain information and data to properly conduct independent audits and examinations, the result is a direct, negative impact on the perceptions of B.C. residents with regard to the effectiveness of policing oversight mechanisms and confidence in B.C.'s justice system. Without an exemption under the FOIPP Act to protect personal information collected from police audits and examinations, PSD is hampered in its ability to make meaningful recommendations that would lead to improvements.

PSD's inability to guarantee confidentiality is also problematic to other oversight functions. For example, the Braidwood Commission of Inquiry recommended that the Province immediately commence a provincial data collection process for the reporting and analysis of 'use of force' data. Under s. 30 for the FOIPP Act, police departments are obligated to protect personal information and have expressed reluctance at providing the full reports to PSD. As a result, PSD's ability to develop a comprehensive 'use of force' reporting and analysis process is compromised. The combination of s. 30 of the FOIPP Act and the lack of exemption for PSD audit records prevents PSD from obtaining valuable data that would contribute to the Province's policing oversight functions. If PSD could guarantee confidentiality of these reports, departments would be more likely to comply fully with the recommendation.

FOIPP Act Challenges:

Current information disclosure requirements under the FOIPP Act result in the reluctance of individuals to provide full information during police audits and other oversight functions. A key aspect in maintaining public confidence in B.C.'s justice and regulatory systems is to ensure the accountability of the police. A critical element to providing this accountability is through oversight mechanisms whereby police activity can be effectively monitored, examined, and scrutinized.

Information, which is often of a private or confidential nature, is essential to PSD's oversight and audit functions as it relays key aspects of the impetus behind and conduct of police actions and, subsequently, how the public interprets the validity thereof. PSD's records are not exempt from the FOIPP Act in the same way as the Office of the Police Complaints Commissioner's records; all PSD records are open to scrutiny and any information or data is subject to access requests under the FOIPP Act. This means that PSD cannot guarantee confidentiality or anonymity to individuals and departments who contribute information during inspections, audits, studies or reviews. Although it is recognized that the Office of the Police Complaints Commissioner is an officer of the legislature and subject to different structures and powers, the functions carried out by PSD also result in information that is highly sensitive in nature. Under current FOIPP Act requirements, PSD is hampered in its ability to:

- Have an early warning system in place to manage risks related to policing oversight;
- Effectively make recommendations for policing standards, policies or training; and
- Ensure adequate and effective levels of policing in B.C.

The inability to guarantee confidentiality invokes serious concerns among individuals and departments about providing information to PSD. This compromises PSD's ability to fulfill its oversight and audit functions, which jeopardizes the ongoing provision, and perceptions of a robust and effective justice system for B.C. residents. Essentially, this has negative implications for the citizens of B.C. as they cannot be confident that adequate and appropriate steps are being taken to achieve police accountability or enhance police effectiveness.

Proposed Remedy:

- Disclosure: Suggest a new s. 15.1 to exempt any records generated from *Police Act* audits and examinations. The Police Complaints Commission has such protection under s. 66.1 of the *Police Act*. The amendment for police audits and examinations should be similar to s. 66.1 such that any record arising out of or related to *Police Act* ss. 40, 42, 43 and 44 (review, study, audit and investigations of the Director of Police Services) would be exempt.

  OR

- The remedy could be constructed more generally to cover government research, audits, studies or reviews conducted to inform programs for continuous improvements or performance measures but with the goal of keeping sensitive information and identity of participants confidential.

Benefits to Citizens:

Integral to PSD oversight functions, which are inexorably linked to maintaining the confidence of B.C. residents in the province's justice system, is the ability to collect information and data whether from police departments or through surveys and interviews of key individuals related to the aspect of policing being examined. Participants include police officers, police administrators and executives, people who have submitted complaints against police, victims of crime, and other vulnerable groups.

Effective PSD audits rely on critical information that may be blunt or quite direct, but which is provided without fear of consequences. Without candid information from participants, the information upon which audits are based will be limited. Limiting the transmission of key information relating to policing accountability to oversight agencies would be of serious concern to the residents of B.C., who expect audits and similar functions to be performed with a high level of integrity.

Police oversight by government is the foundation of citizens' trust and support for policing and justice systems. Ensuring the functionality and integrity of government's oversight mechanisms, such as police audits, is a key aspect of fulfilling citizens' expectations that police accountability remains uncompromised.

Challenge #7: *Freedom of Information – Limited Timelines to Respond to FOI Requests under the FOIPP Act when a Government Body is Undertaking to Provide a Public Report*

Problem Description:

The Ministry of Public Safety and Solicitor General receives numerous access requests under the FOIPP Act. Some of those requests involve information that will be contained in a future public report. Often these requests for information are received before the preliminary data is analyzed and the report is drafted.

FOIPP Act Challenges:

Under the FOIPP Act, access requests must be responded to within time limits. Often the same staff are tasked with both drafting a public report for release and responding to access requests. Therefore, work on the report is often delayed while staff take time

to respond to the access request related to the same subject matter. Issues arose for the B.C. Coroners Service when the Ministry undertook to examine the issue of the files missing after the Children's Commission was wound down. Had the Ministry been able to complete the study and publish the resulting report first, numerous access requests each requiring individual attention, could have been satisfied by the public report instead. The issue with s. 20 of the FOIPP Act is that the section applies to a report that is to be published within 60 days but does not apply if publication will take place within any other time frame. If the end product is a public document, limited government resources could be directed toward the timely publication of a document for public viewing rather than responding to the access requests concerning the information.

Proposed Remedy:

- Disclosure: Suggest amending s. 20 to more properly reflect the time it takes to compile a report for publication. The time period could be specified to be different lengths depending on the scope of the study or inquiry, which depending on the type of report could be between 3 to 6 months.

Benefits to Citizens:

Dedicating resources to completing studies and reports in a timely manner benefits the people of British Columbia who want a transparent and accountable government. The arrival of numerous access requests on the material to be contained in a future report, impacts resources and service delivery to the public. The proposed amendment would allow resources to be directed to drafting a more timely public report or responding to other access requests.

Challenge #8: *Freedom of Information - Court Records*

Problem Description:

Court records are outside of the scope of the FOIPP Act as the collection and distribution of court records are governed by legislation, court rules and orders, and judicial policy. Court records are excluded from the FOIPP Act as "record in a court file". The term "record in a court file" is not defined in the Act and neither is the word "file". The term "record in a court file" was incorporated into the legislation at a time when paper records were the norm. The development of electronic information systems has resulted in the potential to create, distribute and access court documents in ways that were not contemplated at the time legislation such as the FOIPP Act was developed.

In the absence of jurisprudence on the definition of the term "record in a court file", there are three ways in which electronic court records might be considered to fall within the scope of the FOIPP Act:

1. Electronic court records are not contained within a traditional paper court file. A narrow definition of "file" will draw these records into the scope of the FOIPP Act.
2. Views or print outs of electronic court records may be considered "copies" and subject to the provisions of the Act.

3. Information contained in electronic court systems can be grouped and displayed in ways that go beyond what is traditionally contained in a paper court file. A narrow interpretation of "record in a court file" may not cover these new ways of accessing court record information and draw court records into the scope of the legislation.

The Ministry and the judiciary are moving toward a wholly electronic court record. If the OIPC finds that electronic court records fall within the scope of the FOIPP Act, this will create significant problems of access and timeliness in the administration of the court systems. Further, it will limit or prevent advances in the court process.

FOIPP Act Challenges:

While "record" is broadly defined, the lack of a definition for the term 'record in a court file' leaves open for debate whether a record is only information contained in a paper file. This interpretation, if adopted, would call into question the nature of the data and documents created, stored and managed through courts' electronic systems. If that were the case, the possible result would be that some electronic information would be subject to the FOIPP Act, but some would not be. Such a situation would present significant problems, not the least of which would be limited access to court record information for all persons involved in a court process. It would also have significant cost implications for the Ministry and, likely, for members of the public seeking access to records.

The court record is not, and never was, limited to documents within the file folder. The term "record in a court file" is inaccurate and does not characterize the true nature of court records, particularly court records in the electronic world. While the FOIPP Act has not yet prevented initiatives from moving forward, a narrow interpretation of "record in a court file" would have significant and far-reaching effects on the court process, on justice partners, and on the public including the media.

> ***Example: Court Services Online*** *- Court Services Online is a service that provides access to court record information and electronic filing services, displays data that, pursuant to judicial policy, is public court record information. These policies have been developed with privacy and access principles in mind. If the Act were found to apply to Court Services Online, the principles of the Act would require changes to the court system. In the interim, it may require the system to be shut down. This would affect the access of the public to court record information and to registry services. It would affect access by defense counsel, victim services and others who use Court Services Online for current information such as appearance dates. It would also affect members of the media who are regular users of the courts' electronic information systems*.

Proposed Remedy:

Change the term "record in a court file" in the FOIPP Act to "court record" and include the following definition of "court record" in Schedule 1 of the FOIPP Act:

"Court record" includes, whether in an electronic form or otherwise:

- *All documents, information and things (which includes any device by means of which documents, information and things are recorded or stored) collected, received, prepared, maintained or archived by or for a court or its staff in connection with a proceeding (including any reports, lists or indexes, generated from such documents, information or things); and*
- *All case-specific information contained within a case management and/or case tracking system (including party names, case status, appearances, and dispositions) and any individual or general reports generated from a case management or case tracking system.*

A definition would provide certainty for the Ministry that the systems, developed in conjunction with the judiciary, will not be challenged as being under the scope of the FOIPP Act.

Benefits to Citizens:

The courts' electronic information systems are providing greater opportunities for citizens to access court record information and to participate in the court process. Citizens can view court record information from remote distances and at any time of the day. Citizens can file court records from remote locations, eliminating the need to travel to the court registry in many cases. The court systems improve the access of registry staff to court record information for the purposes of managing the record. This allows for business efficiencies that could not be realized before and new workflow processes that maximize resources.

Other benefits include increased and timely access to court records for judges, police and other justice partners. The downstream benefits of the timely transfer of information amongst justice partners include safer communities and stronger citizen engagement with the courts.

Concluding Comments

Several provisions of the FOIPP Act currently create difficulties for staff in justice ministries and contracted service providers to perform their jobs in an agreed-upon, timely and effective manner. These difficulties are experienced whether the sharing of information across agencies to serve a victim of crime, other family member or offender is at issue, or the carrying out of studies, audits and provision of security through surveillance.

Over the years, government has moved away from the silo approach to program delivery towards a more collaborative cross-agency approach to services for British Columbians. It has promoted performance measurement so that government can continuously improve programs. The discussion and examples provided are testimony to the fact that without changes to the FOIPP Act and/or its interpretation, client service delivery will continue to be impacted. What is needed is a modernization of the FOIPP Act to reflect the parameters of government programs, as well as a re-education of government staff to ensure the new freedom of information and protection of privacy rules are understood and easily incorporated into practice. This review represents an important opportunity to achieve those objectives.

Ministry Mandate

The Ministry of Housing and Social Development (MHSD) brings together a number of social priorities and integrates a wide range of services. The Ministry strives to ensure that low income earners and people dealing with homelessness, addictions, mental illnesses and disabilities have access to supports when and where they need them most so they can become independent and participate more fully in their communities.

MHSD is responsible for housing programs and homelessness initiatives, income assistance and employment programs, the Provincial Disability Strategy and supports, gaming policy and enforcement and liquor control and licensing.

The Ministry is responsible for Housing Matters BC under which the Province is investing in housing programs to provide direct housing assistance for individuals and households throughout the province.

Outreach initiatives undertaken directly and coordinated by the Ministry connect homeless British Columbians to needed supports. The Ministry connects people to affordable housing, income assistance, employment programs and mental health and addictions services to help them improve their health and move towards independence.

As part of the Provincial Disability Strategy, MHSD is partnering with local communities to make supports and services more accessible and integrated for British Columbians with disabilities.

Income assistance programs administered by the MHSD ensure that British Columbians who are most in need receive the benefits and supports for which they are eligible. The Ministry is also responsible for administering employment programming for income assistance clients. The transfer of federal employment programs to the Province is now complete and funds are being allocated in a way that best meets British Columbia's unique labour market priorities and the local training needs of clients. Volunteer programs give people an opportunity to develop their skills and contribute to their communities and neighbours. The Province currently invests over $70 million a year in employment programs and the demand for these programs and other related services is increasing.

MHSD is responsible for ensuring the integrity of gaming and promoting responsible gambling practices so that citizens remain confident in how gaming is conducted. Gaming revenues are invested in key social priorities, including health care and education.

The Ministry is also responsible for liquor licensing and control practices to ensure safe and responsible liquor service. Liquor inspections and programs like Serving It Right help protect customers and the community.

Better Outcomes

Challenge #1: *Barriers to Integrated Service Delivery for Vulnerable Populations*

Problem Description:

The Homelessness Intervention Project (HIP) was launched in March 2009. The 18 month HIP project provides services to approximately 2000 homeless individuals in Victoria, Vancouver, Surrey, Kelowna, and Prince George who have been sporadically or chronically homeless for more than a year and who struggle with mental illness and/or addictions.

While MHSD has the lead role in coordinating provincial and community social housing and support services, other project partners include the ministries of Health Services, Public Safety and Solicitor General, Attorney General, Children and Family Development, Citizen Services and agencies such as the health authorities, Community Living BC and BC Housing, as well as municipalities, contracted service providers and the non-profit sector.

One of the goals of the HIP is to identify the chronically homeless and fast-track these individuals to government services and supports.

HIP clients must be supported to enable project partners to easily share pertinent information about the clients they jointly serve. The challenge of information sharing among these partners goes beyond resistance to sharing sensitive personal information. Basic information such as whether a person receives subsidized housing or whether they are a client of a particular agency can be difficult to access. This inability of public bodies to share basic information means that clients have to navigate multiple agencies repeating their stories, providing tombstone and eligibility information again and again. For many clients, who have mental illness or addictions and are without advocacy or familial support, this expectation is unreasonable. This cumbersome approach also creates the potential for overlap of services and for some clients to "double-dip" into services. Without effective information sharing, it is difficult for government to discover cases of overlap or abuse.

Breaking the cycle of homelessness requires an integrated approach to service delivery and information sharing between project partners. Repeat offenders are one example of how an individual can miss an opportunity to be housed if information is not shared between partners. An offender may lose an opportunity to be housed if an opening in assisted housing arises for them while they are temporarily incarcerated and the Ministry of Public Safety and Solicitor General is unable to share this information with HIP partners. As a result, the individual may lose the opportunity for stable housing and end up right back on the street and therefore be more likely to have contact with the criminal justice system again.

In order for homeless citizens to access the multiplicity of government services and information that they need, it is imperative that the government takes a "one-government – one social service" approach to information sharing. It is also important

that clients' information be accessible using updated technology and an Integrated Case Management system to ensure the most efficient administration of government services.

> ***Example*** *- Irene is 45 years old and has been living on the street for 18 months. She is "chronically homeless". She has mental health and addictions problems and she is receiving income assistance. However, because of the different services that Irene requires and the inability of HIP partners to share information about Irene, she is asked to complete several different consent forms. Irene has trouble understanding why she needs to sign so many different forms and is frustrated with the process. Later, it is discovered that Irene is already receiving some services from a not-for-profit agency but because of the inability to share her information there was some duplication of services to Irene.*
>
> *The goal is for Irene's needs to be assessed by the integrated team and for her to sign one consent form that will be shared with all of the participating partners. The Integrated Case Management system will provide a central source of information government can use to ensure Irene gets the right mix of services and supports. It will also enable government to evaluate the success of the services and supports Irene is receiving and to make changes if required.*

The HIP is not the only integrated project to encounter challenges related to the FOIPP Act. From 2006 until 2008 the Disability Alignment Project, a project linked to the Provincial Disability Strategy, attempted to streamline access to disability services for persons with disabilities. With MHSD as the lead ministry, a cross-ministry committee was struck with the intention of creating a one-stop shop for persons with disabilities. The application process that confirms disability status became the focus of the project, namely to integrate the application process between disability service providers to ensure that persons with disabilities would not be required to complete an application for each separate service within the provincial government. The goal was also to make a person's disability status accessible electronically to all government services and programs that serve persons with disabilities. However, information sharing related to the integrated application for persons with disabilities became a significant barrier to moving this project forward. Without a clear definition of what constitutes a common or integrated program in the FOIPP Act, the OIPC determined that an explicit statement from the legislature to confirm that the project was truly integrated was required. Since the project was an initiative under the Provincial Disability Strategy there was no separate budget or governance structure. Without an explicit statement from the legislature, the solution was to manage the project through privacy impact assessments and information-sharing agreements between partners; however, this approach met with restrictive and narrowly interpreted collection and disclosure provisions in the FOIPP Act.

FOIPP Act Challenges:

Part 3 of the FOIPP Act that governs the collection, use and disclosure of personal information inhibits a citizen-centred, one government - one social service approach and severely limits the ability of social service providers to integrate services for citizens. Moreover, as both the HIP and the Disability Alignment Project demonstrate,

the lack of clear language and/or criteria in the FOIPP Act about what constitutes a common or integrated program, has resulted in restrictive interpretations being developed by the Information and Privacy Commissioner's Office and some public bodies. This impedes the progress of innovative projects designed to better integrate and coordinate services to provide enhanced outcomes for clients.

The requirement under s. 26(c) that personal information collected by a public body must relate directly to and be necessary for an operating program limits the ability of functionally integrated project partners to collect information from one another and ultimately improve services to vulnerable people. Furthermore, the requirement in s. 27(1) that a public body collect information directly from an individual is not workable for functionally integrated projects serving vulnerable populations. For example, when each public body within an integrated team requires separate consent forms from the citizen that they are trying to serve, the ability to provide that person with the right combination of services in the most responsive manner is hindered.

Proposed Remedy:

Amend the purpose for which information may be collected (s. 26(c)) and how personal information is to be collected (s. 27(1)(b)) to ensure that functionally integrated project partners have the authority to collect information from one another. One suggestion is to ensure that s. 33.1(b) regarding consent to disclosure is expressly linked to the collection of personal information needed for integrated projects to function effectively. Amendments to the collection of personal information should be written with the unique challenges of vulnerable populations in mind and perhaps even articulated in the Act.

Amend s. 33.2(d) regarding the disclosure of personal information for the delivery of a common or integrated program or activity to clarify what the terms "common or integrated program" mean so that narrow, non-functional interpretations that block innovative service projects do not occur. Personal information should be able to be disclosed to integrated project partners that do not meet the documentation requirements of an integrated project, but who can prove—through executive approval, project charters, or other documentation—that they are functionally integrated for the common purpose of serving the needs of a vulnerable person. One suggestion would be to allow the sharing of information under certain conditions such as if there is an immediate need to meet the health or shelter needs of a client or for the purposes of evaluating an integrated project. The FOIPP Act needs to make a shift from the narrow focus on discreet public bodies to a broader view of interdependent public functions.

The provincial government is currently working to develop integrated case management solutions through new information technology systems. This project could have a profound impact on integrating and improving service delivery for vulnerable people. Amendments to the collection and disclosure provisions of the Act should support an integrated case management system that will improve information sharing among integrated project partners and streamline the administration of integrated government services for vulnerable citizens.

Benefits to Citizens:
If these proposed amendments are made to the legislation, vulnerable citizens who are homeless, for example, will be able to better receive the multiple essential services that they require to remain permanently housed. The collection and disclosure of information within integrated projects will be managed through an integrated case management system allowing for more responsive services and less duplication. These amendments should ensure that a citizen like Irene is off the street faster and is made aware of all of the social services that she may be eligible for. The FOIPP Act needs to enable projects like the HIP rather than acting as a barrier to meeting the multiple needs of vulnerable citizens.

Challenge #2: *Barriers to Project Evaluation*

Problem Description:
In surveying ministry staff about their experiences with the FOIPP Act, a recurring theme was that the complexity of the Act often results in differences in opinions between ministries, and even within ministries, about what information can be shared, when and with whom. Staff report their concern with the significant effort needed to determine if information can be shared between government agencies, the challenge of working with the OIPC and the frustration at having the FOIPP Act impede their work.

Projects that have run into problems include research projects designed to evaluate the effectiveness of government programs on improving the lives of B.C.'s most vulnerable. One such example was the evaluation of the Provincial Homeless Initiative (PHI), a project to assist homeless individuals into supportive housing. The evaluation was intended to identify the impact of supportive housing on the wellbeing of former homeless individuals, including health, crime and poverty measures, as well as identify best practices to improve outcomes. The evaluation framework required the collection and disclosure of personal information by the Ministries of Health Services, Housing and Social Development, Public Safety and Solicitor General, and the regional health authorities. The MHSD Housing Policy Branch was prevented from moving forward with the evaluation as the branch was advised that these project partners only had the authority to disclose the personal identifiers of individuals in two scenarios: 1) Section 33.2(d) (common or integrated program) and 2) Section 33.2(k) (research purpose).

The Housing Policy Branch attempted to move the project forward, first as a common or integrated program or activity and finally as a research project. Ultimately, both approaches were deemed unacceptable under the FOIPP Act.

> ***Example -*** *John Thompson was sporadically homeless for several years prior to entering supported housing under the Provincial Homeless Initiative. John was also served by the Ministry of Health Services for a chronic condition and had interactions with the Ministry of Public Safety and Solicitor General at the same time. Multiple factors contributed to John becoming homeless. Despite several attempts to evaluate John's experience with the PHI, his experience was ultimately not evaluated. It remains unknown to what degree John was successfully served by the integrated approach of the PHI and how he and other homeless individuals could be better served in the future.*

The goal is to assess John's experience with the PHI to ensure that he remains permanently housed and that his health and other needs are simultaneously addressed. In order to effectively evaluate John's experience with the PHI, stakeholders must clearly understand the rules governing information sharing within integrated projects and be able to share pertinent information in a timely way that will ultimately improve how homeless or vulnerable people are served.

FOIPP Act Challenges:

Significant staff resources were dedicated to trying to implement this important project evaluation and understand and interpret the Act and comply with the Office of the Information and Privacy Commissioner direction.

Despite a number of deputy ministers expressing in writing that the PHI was a common or integrated program, the OIPC, based on its interpretation of the legislation, advised that the PHI was not a common or integrated program or activity under s. 33.2(d). In the absence of defined criteria in the legislation to delineate the parameters of a common or integrated program, the OIPC has determined that to be considered a common or integrated program or activity and to proceed with the evaluation under s. 33.2(d), a project would need, among other things, a recorded mandate, budget or plans or comparable "documented structure." The branch took the position that the four ministries and health authority had interrelated mandates to address issues of mental illness, addictions and homelessness. Based upon common interests and mandates, all of these agencies had formed a steering committee to guide the development of the evaluation. However, there was a lack of confidence that the evidence would satisfy the conditions outlined by the OIPC so the branch decided to change course, planning to enter into research agreements with Health, Housing and Social Development, Public Safety and Solicitor General and the regional health authorities utilizing s. 33.2(k) of the FOIPP Act. This approach was also deemed problematic by the OIPC. Attempts to move this project forward were discontinued.

Proposed Remedy:

Similar the first issue described, the Homeless Intervention Project, the proposed remedies with respect to the PHI are similar. It is recommended that amendments be made to ss. 26(c) and 27(1)(b) regarding the collection of personal information and to s. 33.2(d) regarding the disclosure of information in order to support functionally integrated projects and their evaluations.

Moreover, the rules that govern information and data sharing within integrated projects must be clarified in the FOIPP Act in order to avoid conflicts of interpretation.

Benefit to Citizens:

The proposed amendments will improve data sharing across ministries and agencies to facilitate the evaluation of social programs that provide integrated support services for vulnerable populations. Without being able to monitor and evaluate projects like the PHI, government is unable to understand the systemic benefits of permanent housing (and the associated cost-savings) or how to make appropriate improvements to projects to better serve citizens.

Citizen Centred Service

Challenge #3: *Inability to fully utilize services offered by foreign vendors*

Problem Description:
Section 30.1 of the FOIPP Act that prohibits the storage and access of personal information outside of Canada has prevented parts of the ministry from utilizing the services of a variety of foreign vendors and, as a result, has reduced competition and likely resulted in the loss of significant cost savings.

A great deal of Canadians' sensitive personal information (such as their banking information) is already stored outside Canada and this is something that virtually all citizens take for granted in this digital age. Many British Columbians choose to participate and share their personal information through social networking websites that are based outside of Canada. Ultimately, a prohibition that only affects public bodies in B.C. may be ineffective in preventing access to this information under the *USA Patriot Act* and simply impedes the ability of public bodies in B.C. to pursue opportunities to attain goods and services and provide goods and services in a more cost effective manner.

FOIPP Act Challenges:
The prohibition of the storage and access of personal information outside of Canada (s. 30.1) prevents all public bodies from utilizing the services of a variety of foreign vendors and, as a result, has reduced competition and likely resulted in the loss of significant cost savings.

Proposed Remedy:
Section 30.1 of the Act should be repealed, or at the very least, an exception should be made for commercial public bodies, similar to that in Nova Scotia's *Personal Information International Disclosure Protection Act*, which states at s. 5(2):

> *The head of a public body may allow storage or access outside Canada of personal information in its custody or under its control, subject to any restrictions or conditions the head considers advisable, if the head considers the storage or access is to meet the necessary requirements of the public body's operation.*

Benefits to Citizens:
Government will be able to procure the technological tools necessary to conduct its business in a cost effective manner that is competitive with other jurisdictions.

Challenge #4: *The definition of personal information is too broad*

Problem Description:
Another issue is that what constitutes personal information under the FOIPP Act is too broad. A narrower approach to what constitutes personal information makes sense – information that can be found in a phone book or is otherwise publicly available should not be subject to the same strictures as clearly sensitive personal information such as medical, educational, or financial information.

FOIPP Act Challenges:
What constitutes personal information under the FOIPP Act is too broad.

Proposed Remedy:
The FOIPP Act should be changed so that the definition of "personal information" is changed to "private information" (as the FOIPP Act is supposed to be about the protection of privacy and not all personal information is private). The definition of "private information" should be:

- *"a record of a person's name in combination one or more of that person's:*
- *Date of birth;*
- *Government-issued identification numbers;*
- *Bank account numbers;*
- *Credit card numbers;*
- *Biometric information;*
- *Financial transaction information;*
- *Medical information;*
- *Password information; or*
- *Security-related details."*

In fact, 37 US states have definitions of personal information in their legislation that are even more restrictive than that proposed above. Their definitions are all substantially similar to the one below (from New Hampshire):

(a) "Personal information'' means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.
(2) Driver's license number or other government identification number.
(3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(b) "Personal information'' shall not include information that is lawfully made available to the general public from federal, state, or local government records.

Benefit to Citizens:
Will simplify interactions with government and reduce some of the challenges related to information sharing, common or integrated programs and the use of social media.

Concluding Comments

As mentioned previously, MHSD brings together a number of social priorities and integrates a wide range of services to ensure that low income earners and people dealing with addictions, mental illnesses and disabilities have access to supports when and where they need them most so they can become independent and participate more fully in their communities.

In order for the Ministry to best serve the needs of these most vulnerable British Columbians, it is imperative that the gap between the definition of common or integrated program or activity under the FOIPP Act and the operation of functionally integrated projects be closed. The FOIPP Act needs to make a significant cultural shift away from independent government bodies toward interdependent government functions that serve citizens with multiple and inter-related needs. Moreover, the legislation needs to support the use of technologies such as an integrated case management system that enable information sharing among integrated project partners while still protecting the private information of citizens.

The legislation needs to be simplified and made accessible in order to ensure consistency of interpretation between stakeholders. The collection and disclosure provisions within the Act should be amended to support integrated projects that serve the most vulnerable British Columbians.

The case to amend the FOIPP Act provisions regarding restricting storage of information outside Canada takes into account technological developments allowing more efficient and effective service delivery benefiting all citizens. Changing the government's approach to what constitutes personal information to focus on sensitive personal information will enhance the overall privacy protection environment in B.C.

MINISTRY OF CHILDREN AND FAMILY DEVELOPMENT

Ministry Mandate

The Ministry of Children and Family Development (MCFD) promotes and develops the capacity of families and communities to care for and protect vulnerable children and youth, and supports healthy child and family development to maximize the potential of every child in B.C.

MCFD is responsible for regional and province-wide delivery of services and programs that support positive and healthy outcomes for children, youth and their families. In order to effectively and efficiently deliver services and programs, MCFD is organized into five regions: North, Interior, Fraser, Vancouver Coastal and Vancouver Island. MCFD's responsibilities include: family development, early childhood development, services for children and youth with special needs, child and youth mental health, child care, child protection, children in the home of a relative, residential and foster care, adoption for children and youth permanently in care, community child and youth mental health, programs for at-risk or sexually exploited youth, and community youth justice services.

In addition, MCFD is responsible for a number of specialized provincial services such as youth custody, youth forensic psychiatric services, services for deaf and hard of hearing children and youth, and the Maples Adolescent Treatment Centre.

MCFD serves children, youth and families either directly or through community service agencies. MCFD's service delivery partners include: contracted service providers, other ministries, family foster homes, Aboriginal and non-Aboriginal communities, delegated Aboriginal child welfare agencies, school districts and health authorities.

MCFD provides a wide range of voluntary and mandatory services under the *Child, Family and Community Service Act (CFCSA)*, *Adoption Act*, *Youth Justice Act*, *Youth Criminal Justice Act (Canada)*, the *Child Care BC Act*, and the *Child Care Subsidy Act.*

MCFD is committed to its role through the *Strong, Safe and Supported* operational plan that details the actions MCFD is taking to provide better outcomes for B.C.'s children and youth. Initiatives include the Integrated Framework for Children and Youth, the Early Childhood Screening Program, Strong Start, Children and Youth with Special Needs Framework for Action, and the Children's Education Fund. MCFD is also introducing changes in response to the Hughes Review and other reports that recommend finding ways to break down barriers to information sharing.

Appropriate and timely information sharing is key to achieving the enhanced co-ordination and cross-ministry work necessary for this long-term plan which requires MCFD to increasingly move away from a program specific service delivery model to a holistic model based on the service or activity pillars of (1) prevention, (2) early intervention, (3) intervention and support (individual assessment and planning), (4) aboriginal approach, and (5) quality assurance.

Better Outcomes

Challenge #1: *Integrated Programs and Proactive Information Sharing*

Problem Description:

The current FOIPP Act s. 33.2(d) integrated program definition does not support the MCFD vision of a family support service continuum which sees information passing from ministry to ministry and other bodies promoting delivery of services that are specifically tailored to the strengths and needs of the individual.

Information collected or created regarding an individual in relation to one service could often inform delivery or enable co-ordination of another service. Establishing cross-services programs as "integrated" and linking this information based on the identity of the individual, as demonstrated in the following scenario 1, could drastically improve the appropriateness and responsiveness of services citizens receive and ultimately improve outcomes for some of British Columbia's most vulnerable population. It is important to note that many of MCFD's clients and contacts lack either the resources or capacity to navigate the complex array of social services provided by many different bodies without "inside" assistance.

Further, the FOIPP Act does not adequately address ad hoc instances where proactive disclosure of information is necessary to support the integration of safety activities aimed at protecting citizens from grave harm as explored further in the following scenario 2.

The need to support integrated service delivery through enhanced information sharing has been identified by Gove, Hughes and Turpel-Lafond as is referenced in more detail under "meeting the needs of citizens" at the end of this section.

Scenario 1—Integrated Case Management (ICM):

MCFD is moving in the direction of Integrated Case Management (ICM) practices. This will require timely access to information from multiple public bodies to support case planning decision making and getting the right services to those who need them at the right time.

ICM as an "integrated program" collects information under the FOIPP Act s. 26(c) and discloses information to integrated program partners in other service areas within and without the ministry under the FOIPP Act s. 33.2(d). With the lack of formal definition of "integrated program" conflicting interpretations will continue to undermine the successful implementation of integrated case management practice and this much needed collaborative services approach.

The scope of information to be shared in the ICM process is the product of a wide variety of services offered by MCFD and other public bodies such as the Ministry of Housing and Social Development (MHSD). Information varies in sensitivity and services range from voluntary (e.g. application for benefits, grants) to mandatory (e.g. ministry initiated child protection, youth detainment). Information is about:

1) persons receiving services (e.g. children in care, youth under special needs agreement, prospective adoptive parents, parent requiring child care subsidy supports, etc.),
2) persons related to the person receiving services, (e.g. birth parent, siblings, relatives, child receiving subsidized child care services), and
3) persons providing services (e.g. foster parents, respite care providers, subsidized child care providers).

Of the persons receiving services, many of these individuals, due to their complex service needs, are often in receipt of services from several different programs and from different public bodies. Further, the individual's connection or relationship to other persons (family) is often critical information in determining services.

Example of family connections and services *- A family on income assistance takes in a relative's child under the Child in Home of a Relative Program (CIHR). Family's two children and the cousin now staying with them under CIHR require after school care and family receives subsidy under Child Care Subsidy programs. An older youth sibling is living outside the household under a Youth Agreement.*

Service/Program	**Legislation**	**Ministry**
Child in Home of a Relative	*Employment Assistance Act*	MCFD but delivered under agreement by MHSD
Child Care Subsidy	*Child Care Subsidy Act*	MCFD
Income Assistance	*Employment and Assistance Act/Employment and Assistance for Persons with Disabilities Act*	MHSD
Youth Agreements	*Child, Family and Community Service Act*	MCFD

To get the right mix of services to the right person at the right time, services must be connected or integrated at the person level and their interconnection to other individuals (family members) across the family support services continuum must be identified. ICM will establish a single cross-services ID placing the individual at the center of services with each service accessing and connecting their service via this single point.

> ***Example -*** *Sara is a 17 year old girl who has recently taken up residence on her older sister's living room couch. Sara has Fetal Alcohol Spectrum Disorder and has dropped out of school recently. Her mother struggles with substance use issues and her father works in construction but has chronic back problems and is currently on income assistance as he is not able to work and he has no work disability benefits. The parents have reached their limit with her lack of motivation, staying*

out all night on several occasions and refusing to find work. Her sister works at McDonalds and makes barely enough to meet her own needs.

Sara's sister has contacted Child and Youth Mental Health (CYMH) where Sara has received support services in the past to report that Sara has been cutting herself again.

Sara and her family are known to a number of services across the family supports continuum, Housing and Social Development, Child and Youth with Special Needs, CYMH, addictions services—but there is currently no information connection between these services, and other service options are not being identified to support Sara and her family.

If a consolidated person ID register model was in place, including current contact information, relevant services within the family support services continuum would (1) know that Sara had moved out of the family household, identifying that Sara may not have sufficient means of self support and potentially impacting parent's income assistance rate, (2) know that mother is receiving addictions services and that father has a chronic health issue, and (3) be able to identify and co-ordinate other supports and services that could benefit each family member (e.g. educational or training opportunities).

Scenario 2—Domestic Violence Notification Protocol:
Proactive notification from and to other services on occurrence of pre-identified critical events (e.g. threats of violence or harm against others made by a youth receiving mental health services) would enable initiation or extension of key services by the notified service to associated impacted individuals.

***Example** - Joshua is a seven year old boy who lives with his single parent mother, Bethany, and 4 year old sister. He has become increasingly aggressive over the past several months—hitting his younger sister frequently and refusing to listen to his mother. There have been complaints about his behaviour at school, but mother believes the school is singling out her child. A few days ago Joshua tried to strangle the family cat.*

Bethany struggles with depression and is being seen at adult mental health services and is on anti-depressants that make her very sleepy. She has shown up at the emergency ward twice in the past 6 month—the first time with a concussion saying she fell down the stairs and the second time with a broken ankle saying she had tripped over toys. The family is on income assistance. Mother has a new boyfriend and a history of relationships with men who are typically unemployed, abusive and end up moving in with her.

Bethany recently contacted and met with CYMH following the incident with the cat. She would like assistance with handling Joshua's behaviour at home and making him listen better. The CYMH clinician notices that mother has fresh bruises on her arms and is walking with a limp. Bethany does not share the information that these injuries are the result of a recent domestic violence incident involving her new boyfriend and that the incident was witnessed by Joshua.

Currently, CYMH has no way of knowing the family's history with other service providers unless the mother gives this information. It is possible that there is current or historical family violence, child welfare or other involvements where a possible grave harm could threaten or impact the child's, his sibling's or his mother's safety or well being. CYMH offers services responsive to the limited information provided by the mother.

If a proactive notification process where in place, the local municipal police force would have notified MCFD (because children are in the household) and other relevant social service continuum providers of these three domestic violence incidences over the last six months, and supports and services to Joshua and his family would better reflect the more comprehensive picture of household life.

FOIPP Act Challenges:

Integrated citizen centric activities described in the above scenarios represent a very significant shift in how a public body, as service delivery partner, defines a "program" and how collection, use and disclosure of information is managed.

- Control of records shifts from the program that collected the information to them being mutually controlled by all programs that have access to the records in order to provide coordinated services to citizens. The FOIPP Act assumes a public body has records management control of the information and is responsible for disclosure decision making about the information.

And

- Use for consistent purpose becomes very broadly interpreted to reflect the wider group of partners who will use the information to deliver their own consistent purpose but specialized services to the individual. The FOIPP Act requires that each public body use personal information only with the consent of the individual, for the purpose it was disclosed to the public body under ss. 33 to 36, or, for the purpose it was collected or for a reasonably or directly connected purpose.

Proposed Remedy:

Integrated Program

To make ICM and other cross-public bodies integrated activities work under the FOIPP Act s. 33.2(d), all of the following FOIPP Act issues must be addressed:

- *"integrated program" undefined*—legislation is currently silent on a definition of "integrated program".
- *Remedy:* Define integrated program in the FOIPP Act schedule 1

And

- *"integrated program" does not identify which service partner/public body has records management control of the personal information*—yet FOIPP Act ss. 30, 30.1, 32, 33, 35 and 36 all reference the public body's responsibility to manage information in its control in a particular manner.

Remedy: Assign control of the information to the integrated program instead of a public body. Appoint an information steward to be responsible for information management balancing the interests of all partners.

And,

- *Compelling authority to collect or disclose within the ICM "integrated program"*—In ICM, the collective ownership described in 2 above, does not apply to the detailed service case file. Control of this portion of the client's family support services file remains the responsibility of the service provider. Selective information sharing with other ICM partners of this case specific detail is required to support service delivery yet the legislative authority to disclose does not exist within the FOIPP Act for programs subject to the Act.

  Remedy: Establish in the FOIPP Act Part 3 comparative authorities to the *Child, Family and Community Service Act* (CFCSA) s. 96 authority for compelled indirect collection and CFCSA s. 79 disclosure without consent when there is an underlying recognition of impending harm to a person's safety or well-being. While the FOIPP Act s. 33.1(1)(m) allows the public body head (deputy minister) to disclose information in compelling circumstances that affect anyone's health or safety, and requires that notice be mailed to the last known address of the individual the information is about, this new CFCSA comparable authority would empower the (delegated) worker to make the disclosure decision and not require notification.

And

- Address how collecting bodies not subject to the FOIPP Act are authorized to indirectly collect this information to maintain parity with the FOIPP Act s. 27(1)(b) provision, and, how these bodies use and disclose information to maintain parity with the FOIPP Act provisions of ss. 32 through 34.

AND

Proactive Disclosure

The Domestic Violence Protocol scenario or other situations where the receiving partner is not otherwise aware of other relevant information would be enabled under the current FOIPP Act provisions IF any one of the following minor changes to the FOIPP Act were made:

- *FOIPP Act s. 33.1(f) or s. 33.2(e) expanded to encompass "possible grave harm" and "protection of the health or safety of a "citizen", changing " … officer, employee or minister" to "person".* This is a conceptual shift that would take this provision from applying internal to public bodies to generally applying to all persons.

Or

- *FOIPP Act s. 33.1(m)(i) "compelling" was broadly defined as inclusive of "possible grave harm" not requiring notification to the individual of the disclosure pursuant to s. 33.1(m)(ii)*

Or

- *FOIPP Act s. 33.2(i) the definition of "law enforcement" included "prevention of domestic violence".*

Benefits to Citizens:
It is government's responsibility to ensure that the right services get to the right persons at the right time. To ensure that both services and funding are being maximized to the benefit of all citizens, this means being able to verify an individual's eligibility for services, being able to direct that individual to other relevant services, and to provide a comprehensive plan of service across public bodies. Enhanced information sharing opportunities through the revision of the FOIPP Act as described above, in conjunction with a review of other provincial legislation containing privacy provisions (beyond scope of this submission), will enable government to more effectively deliver collaborative and citizen responsive services.

The following examples highlight the need for information sharing:

The Honourable Judge Thomas J. Gove (The Gove Report), the Honourable Ted Hughes, Mary Ellen Turpel-Lafond, B.C. Representative for Children and Youth and others have identified the need to proactively share information with those service providers who may be providing services to impacted individuals or families.

BC Children and Youth Review (Hughes), Recommendation 60, "The [MCFD] needs to ensure that no legislative or operational barriers remain to block the sharing of information across its program areas."

No Private Matter: Protecting Children Living With Domestic Violence (Turpel-Lafond) "Contributing factors to an uncoordinated response by the systems involved included:

- inadequate communication and collaboration between MCFD and police, and
- the lack of consistent policies and tools for responding to domestic violence situations between all of the systems."

Citizen Centred Service Delivery

Challenge #2: *Information Sharing to Support Necessary Public Body Partnerships*

Problem Description:
To provide the most benefit to citizens and enhanced service delivery, there are a variety of circumstances where information collected for one purpose would support another purpose or use. However, the FOIPP Act, s. 33.2(a) consistent purpose test, does not allow for such disclosure by the source where the receiving party cannot demonstrate a reasonable or direct connection to the source's purpose for having the information (s. 34). In addition, s. 27(1)(b) only authorizes indirect collection (i.e. the collection from a source other than the individual the information is about) in limited circumstances.

Scenario 1—Consolidated Person Identity Management:
Providing citizens with a system of services where they only need to provide their identification once when accessing multiple social services that cross public body boundaries would enhance the client experience in dealing with government by reducing the amount and repetition of information that would need to be supplied by the individual in order to obtain services. An operational benefit is that all individual involvements and services are connected at the moment of collection and are immediately accessible to others with the demonstrated legal need and right to know which eliminates gaps and overlaps in services.

Not linking services to the individual at time of initiation significantly impacts the availability of information and MCFD's timeliness for accessing information that provides critical detail to inform crisis decision making such as the removal of a child from a home and establishing alternate care arrangements.

> ***Example -*** *Jane Jackson receives child care subsidy for her son Liam from the MCFD Child Care Subsidy program for the 3 days a week when she attends a local community college. Liam Jonathan Smith, age 4, has a medically diagnosed special need. Jane contacts MCFD, Special Needs program to seek support services.*
>
> *With no knowledge of other services being received, the Special Needs resource worker collects all relevant personal details of mother and son from the mother and requests a copy of the doctor assessment of permanent disability. Jane doesn't say anything, but wonders if the proof of disability she provided for the child care subsidy special needs supplement isn't the same thing? The mother obtains a new disability assessment and feels horrible for subjecting her child to yet another assessment process.*
>
> *<u>If a consolidated person ID register model was in place</u>, in which both Jane and her son are already identified, Jane would only have needed to provide her name and date of birth and verify the address on file to open a new Special Needs file. Liam's name, and date of birth would also be verified against information already on file while all other relevant information, including the assessment of permanent disability would be automatically linked to the new file type.*

Scenario 2—Privacy Breach Notification:
The ministry is responsible for notifying individuals whose information has been compromised. The contact information on record may not reflect current location of an individual and accessing more current contact detail from another service provider is not considered to be use for a consistent purpose.

> ***Example -*** *In a recent privacy breach incident MCFD was unable to contact some of the individuals to notify them of the compromise of their personal information, the potential impact to them as an individual, and mitigation strategies.*
>
> *The inability to provide notification hinged on the lack of current contact information held by MCFD as the records that were subject to the breach were dated. A request for access to more current contact information from HSD would have required the disclosure of individual identification to enable data matching*

and was denied as the purpose for MCFD's collection was inconsistent with the purpose for which HSD collected the information.

Scenario 3—BC Early Hearing Program:
MCFD often partners with other public, federal and private sector bodies in serving a mutual client group where each partner has a different contribution or interest within the partnership. In situations where MCFD is block funding a service, return of individual service detail is not required in the terms of the service contract. However, in some cases other MCFD partnership partners may have a significant requirement in the information.

Example - *If implemented, the BC Early Hearing Program, is a provincial program that will provide coordinated, equitable, accessible, efficient and effective early identification and intervention services for children aged birth up to five years of age who are deaf or hard of hearing, and for their families. The program's goal is to enable the identified children and their families to acquire communication skills critical for a child's positive social development, educational achievement and personal independence thus influencing the best possible outcomes for children with congenital hearing loss. The program will be delivered and managed through existing infrastructures of the Provincial Health Services Authority (PHSA), BC Children's Hospital, MCFD, Regional Health Authorities, and contracted service provider agencies and other independent private health service providers. Partnership and consultation with physicians, families, community agencies, service providers and universities is integral.*

In order for the program to be successful, client specific service information consolidation needs to occur across the sector to benefit those individuals in achieving a seamless hearing health services continuum regardless of service provider. Consolidation of information further supports research and analysis of programs and assists in the identification of trends and development of new more responsive services benefiting all citizens.

PHSA is requesting that the client specific service records of MCFD contracted service providers be directly entered into the Ministry of Health BEST database. This information sharing does not meet the criteria of the FOIPP Act s. 33.2(a). (1) it is not in the control of MCFD as per terms of contract, and, (2) if it were, the use of the information by the other partners who have shared access to the database, while reasonably connected to MCFD'S purpose of collection (s. 34(1)(a)), does not, meet the second part of the test (s. 34(1)(b)) of being necessary for performing the partner's statutory duties or operating an authorized program.

Consolidation of early hearing records would benefit the client by creating a subsequent opportunity for MCFD to leverage this information for other over age 6 hearing services. As the FOIPP Act stands now, the information cannot be disclosed as proposed and the segregation of early hearing records continues.

FOIPP Act Challenges:
The authorities for use of personal information under s. 32 of the FOIPP Act do not permit the kind of use that is necessary to successfully operate a multi-partner program. The FOIPP Act also requires that information sharing outside the immediate area of primary collection be supported by an authority to disclose (the FOIPP Act ss. 33.1 and 33.2), AND where the collecting party is subject to the FOIPP Act, be able to demonstrate their authority to indirectly collect the information (s. 27(1)(b)). All of these authorities are deficient.

The information sharing described in the above scenarios shows clear benefit to citizens, yet the authority to disclose, for these purposes that are inconsistent with the original purpose of collection, does not exist.

Information sharing relationships involving parties not subject to the FOIPP Act (e.g. federal bodies, private sector partners, self-governing First Nations) have an additional layer of complexity.

Proposed Remedy:
To overcome these challenges, possible changes to the FOIPP Act could include:

- *replacing s. 33.2(c) "the" public body, thereby limiting disclosure to within the public body, with "a" public body, allowing for inter public body disclosure.*

And

- *changing the consistent purpose connection test of s. 34(1)(a) from "and" to "or" making "necessity" on its own a valid basis for use.*

And

- *addressing how collecting bodies not subject to the FOIPP Act are authorized to indirectly collect this information to maintain parity with the FOIPP Act s. 27(1)(b) provision. And, address how these bodies use and disclose information to maintain parity with the FOIPP Act provisions of ss. 32 through 34.*

Benefit to Citizens:
Expanding the definition of consistent purpose to allow the sharing of information for common reasons to support necessary public body partnerships allows for timely, efficient and enhanced service delivery to citizens. It would enhance the ability of government to provide seamless and coordinated service delivery and mitigates multiple demands on citizens to provide the same information by facilitating the sharing of client specific service information between public bodies.

Stronger Engagement

Challenge #3: *Social Media Disclosure Opportunities and Storage Within Canada Requirement*

Problem Description:

Ministry staff have identified the use of Facebook and other social media tools as a method to engage today's youth on their own terms, enabling the establishment and continuation of communication with individuals who may be difficult to access through traditional methods of communication. While practice will minimize the scope and sensitivity of personal information involved, any communication via a social media site involves disclosure of government information to the third party service provider and that information being stored outside of Canada as most, if not all, social media sites operate in other jurisdictions.

Scenario 1—Family Finders:

The goal of this program includes connecting children with relatives and positive role models who can provide healthy long-term family relationships as the child transitions out of MCFD's care.

> ***Example -*** *The Family Finders Social Worker has been asked to locate relatives of a child in care as part of the permanency planning process. The child in care is a Continuing Custody Order ward and has no current family or long-term relationships in his life. Through Facebook, the Social Worker locates an individual who they believe to be an uncle in Alberta. Additionally, several other possible relatives are also identified through the Facebook search, including cousins and other aunts and uncles. The Family Finder Social Worker reviews local telephone directories in an effort to establish contact off-line. There is no listing. E-mail or "message" contact of the individual via the social media tool of Facebook is the only available option to connect and potentially place child with a blood relative.*
>
> *Family Finder Social Workers would like to have the opportunity to send a general message via Facebook to potential family members, advising that they may be the relative of a child in our care and asking the individual to contact the Family Finder Social Worker by telephone. No client personal or identifying information is shared through this initial Facebook contact.*
>
> *Despite the numerous promising leads, none of the possible relatives make contact with the ministry by phone or respond by e-mail. The ministry, unable to establish contact places the child with a non-relative family and the connection opportunity with blood relatives is lost.*
>
> *If dialogue was allowed in the environment in which the individual located is comfortable (i.e. Facebook), the outcome could have been significantly different.*

Scenario 2—Child Welfare:

The goal of this program includes maintaining contact with children, youth, parents, foster parents and others involved in a child's plan of care.

> ***Example -*** *A guardianship worker has found it difficult to maintain the necessary contact with the youth on her caseload. Scheduling meetings and getting a youth to attend is a challenge as these youth often have busy social schedules, tend not to want to visit offices, are hard to reach by phone, and, could be absent without leave from their foster homes. Further, the urgency of maintaining contact increases where the youth places his or herself in high risk situations.*
>
> *Whatever the youth's reason for not staying connected through traditional methods of communication, the youth might still look to engage or stay in contact through social media, giving the guardianship worker a way to provide support and intervene when necessary to do so.*
>
> *With maintaining communication with the youth on her caseload as the goal, the guardianship worker asks each of the youths for their preferred method of contact. Some youth provide email addresses, some youth provide cellular phone numbers for text messaging, some youth provide MSN nicknames, and some youth prefer to receive messages through their Facebook account.*
>
> *The guardianship worker, always aware of the sensitivity of the information being exchanged through these on-line communication tools minimizes the personal content of outgoing communication but has no control of the youth's content or management of the information. As part of communicating through these media, the guardianship worker strives to raise the youth's awareness and action in protecting their own on-line privacy.*
>
> *Where the third party social media service provider stores information outside of Canada, with the FOIPP Act storage in Canada requirement, the guardianship worker cannot currently engage the youth by their preferred method of communication. This could result in a breakdown in contact.*

FOIPP Act Challenges:

Disclosure and Storage

While disclosure in the provided examples may occur under s. 33.1(c) of the FOIPP Act as the *Child, Family and Community Service Act* (CFCSA) s. 79(a) provides for the opportunity to disclose without consent where the safety or well-being of a child is at issue, the CFCSA will not apply in all cases where use of social media and other internet sites would be of assistance. For these other cases (e.g. a Child and Youth Mental Health clinician communicating with a youth client), the FOIPP Act s. 33.1 (disclosure inside or outside Canada) has no clear opportunity for disclosure through social media or other internet based sites for the purpose of conducting outreach activities and connecting with citizens for service related purposes.

MCFD outgoing communication using social media is disclosure of personal information.

While best practice can minimize the extent of personal information contained in the communication, record of the communication itself links the correspondent to MCFD as a potential client, which reveals personal information about the individual thereby posing a potential privacy harm to the individual.

As web based e-mail servers and internet applications such as Facebook store information outside of Canada, the requirement of the FOIPP Act s. 30.1, which states that information under MCFD's custody or control be stored and accessed in Canada, cannot be met.

The requirement to store personal information inside Canada only resulted from a concern that citizens' data could be accessed through the *USA Patriot Act*. While this concern is real, it is difficult to see how the information in question would be of any relevance to US national security and therefore is unlikely to be accessed by the US Government under the *USA Patriot Act* or any other government under similar legislation.

Proposed Remedy:

- *Add* a provision to the FOIPP Act s. 33.1 to enable disclosure of personal information inside or outside of Canada for the purpose of enhancing engagement with citizens.

  And,

- *Refine* the FOIPP Act s. 30.1 to address storage of information intended for a first party but exposed to and stored by a third party social media service provider.

Benefits to Citizens:

Enabling ministry workers operational use of new technologies and internet tools will enhance the ministry's capacity to connect individuals with services aimed at promoting positive outcomes for children, youth and families. The status quo is a missed opportunity, and as both scenarios above describe, could result in significant impact or consequences to the individual.

Ministry Mandate

Health Sector Stewardship Mandate

The Ministry of Health Services has overall responsibility for ensuring that quality, appropriate and timely health services are available to all British Columbians. The Ministry of Healthy Living and Sport was created to help British Columbians lead healthier lives, and works to enhance the focus and integration of public health programs, services and information by supporting a strengthened and renewed public health system and increasing long term sustainability of the health care system (for a fuller description of the mandates of the Ministries see the Appendix at the end of this section).

The ministries perform their leadership role through the development of social policy, legislation and professional regulation, through funding decisions and fiscal management, and through an accountability framework for health authorities and oversight of health professional regulatory bodies.

The Ministry of Health Services funds health authorities as the organizations primarily responsible for health service delivery. Five regional health authorities deliver a full continuum of health services to meet the needs of the population within their respective geographic regions. A sixth health authority, the Provincial Health Services Authority, is responsible for managing the delivery, coordination and accessibility of selected province-wide health programs and services. The Ministry provides leadership, direction and support to these service delivery partners and sets province-wide strategies, goals, standards and expectations for health service delivery by health authorities.

The Auditor General of British Columbia described this important stewardship/governance role as it relates to Home and Community Care in his 2008/2009 Report *"Office of the Auditor General of British Columbia Home and community care services: meeting needs and preparing for the Future*":

> *The Ministry of Health Services currently allocates about $2 billion annually to five regional health authorities to deliver home and community care services to more than 100,000 clients. As the steward of the health system, however, the ministry has the lead role in setting the strategic direction for the home and community care system, planning service delivery in coordination with the health authorities, and monitoring and reporting on the performance of this aspect of health care.*

The Ministry of Health Services holds the same role for acute (hospital) care, PharmaCare, and other levels of care in the overall health sector.

The World Health Organization (Regional Committee for Europe, Fifty-eighth Session Tbilisi, Georgia, 15–18 September 2008) described a stewardship/governance role as

> *... a core function of health systems which requires specific attention. Increased transparency and accountability are driving forces behind better health system performance, which health system "stewards" strive to achieve by carrying out a number of subsidiary functions: formulating strategies and policies to ensure the attainment of health system goals; gathering and applying intelligence; exerting influence through coordination with partners and other sectors and advocating for better health; ensuring good governance in support of the attainment of health system goals; ensuring that the system can adapt to meet changing needs; and mobilizing legal, regulatory and policy instruments to steer health system performance.*
>
> *Health ministries and governments are moving from a managerial role, directly involved in the delivery of services, to a role of strategic over-viewer making increasing use of incentives and various policy tools to steer the health system towards better performance. The importance of the health and health system stewardship role is also a consequence of the lessons learned from other countries inside and outside Europe and from the successes of different industries and public administrations.*

Personal Information Required to Fulfill Stewardship Mandate

Individual-level data is a key business requirement of the ministries. Individual-level data is data about individual people, and constitutes personal information under the FOIPP Act, even when obvious identifying elements such as name and address (which are not used unless absolutely necessary) have been removed.

Individual-Level Data Required for Accountability and Funding Purposes

One of the most important activities of the Ministry of Health Services is to ensure budgetary accountability to the public. To do so, the Ministry sets specific service levels and outcomes for Health Authorities, and funds them based on their ability to demonstrate that they have met these expected performance targets. This population based, pay-for-performance model often relies on individual-level data reported from Health Authorities to validate that performance-based targets have been met, to monitor and supervise Health Authorities' activities, and to appropriately fund them for the services they provide at the direction of the Ministry. Although much of the data analysis work of the Ministry is reported using aggregate information, the underlying data that produces the final report must utilize individual-level information to enable, for instance, reconciliation between hospital usage, Medical Services Plan, Continuing Care, PharmaCare and other data on a "client-centered" or individual level.

An example of where the Ministry uses individual-level data for accountability purposes is the "30-day follow-up requirement". To make sure the patients with a mental health diagnosis who are discharged from hospital get proper support, the Ministry requires that Health Authorities provide follow up care in the community within 30 days of discharge. Individual-level data must be used to confirm whether this follow-up care is provided. Data must also be collected and used at a provincial level, from all health authorities, as it is possible that the follow-up occurred outside the health authority

responsible for the hospital discharge, and health authorities may not have access to each other's data.

Individual-Level Data Required for Health Care Planning and Improvement Purposes

The ministries also need individual-level data to plan an appropriate mix of services across the province to meet citizens' needs. For instance, a key national and provincial goal (based on the results of a large-scale, national Angus Reid survey) is to increase the number of natural deaths that occur at home, or in home-like settings as opposed to institutional ones. Hospice palliative societies tell us that there are some core components and ideal suites of services to support this kind of care. One of the health authorities has adopted this approach, and has invested millions of dollars in a specialized hospice palliative team that supports end of life care across the region. Yet that same health authority has the lowest rates of home deaths in the province. We need to understand why this has occurred and how it can be addressed.

Another example of where individual-level data is required is to address the very high proportion of seniors in acute (hospital) care who require placement in alternate levels of care (e.g., long term, home or residential care) before they can be formally discharged from the hospital to make beds available for other patients. We know that seniors' functional capacities decline exponentially when they are in acute settings longer than two to three days. What we need to know is, to what degree does this impact the demand and wait times for residential care services; and, are there home health programs or service alternatives that could support seniors to return home and remain independent?

To answer these questions, the Ministry needs to link individual-level information across disparate systems such as home and community care, acute (hospital) care, Medical Services Plan and PharmaCare, as each of these databases contain information about services provided to the same individuals at different times and places, and to address different health needs. In the palliative care example, we may need to understand whether there are differences in the demographic or social factors, or the medical conditions of patients in the palliative care program, compared to other individuals in the province, which lead to the unexpected results. In the seniors' hospital use example, we need to assess how access to care in one setting might impact on access to care in alternate settings, as well as the degree to which geographic or other factors have a bearing on health outcomes. This type of analysis can only be done by linking individual-level information at different levels, and across the province, to ensure patient migration and patient transfers are taken into account.

FOIPP Act Issues

At present, almost fifty percent of British Columbia's budget is spent on health care. Within the current FOIPP Act privacy protection structure, where the health sector is divided into a large number of independent public bodies, the ministries' ability to collect the individual-level (personal) information needed to responsibly manage this budget, and to provide effective health sector governance and stewardship, is challenged to a critical level. Within the health sector as a whole, delays and barriers to information sharing impede management of health services, innovation and cost-saving opportunities and good management of resources. One way to describe trying to

operate in this environment is to see it as a series of artificial "borders" between entities engaged in a common service objective. Before each border can be crossed, your information "passport" (your authority) must be scrutinized and approved; and, even if the information is approved to enter, there has been a delay in crossing the border.

The ministries of Health Services and Healthy Living and Sport are committed to the important trust of maintaining a high standard of protection for the personal information in their care. However, the ministries believe a different "governance regime" that better reflects the contemporary realities of the health system can help them to better meet this responsibility. The ministries recommend that the FOIPP Act "open the borders" between health public bodies to reflect the concept of an integrated health sector in which artificial barriers to indirect collection, use and disclosure of individual-level information are removed.

Challenge #1: *Ministries unable to collect individual-level information from Health Authorities*

Problem Description and FOIPP Act Challenges:

When the FOIPP Act was passed in 1992, the model of government and the approach to delivering government services was substantively different than today. Government services were organized and delivered under relatively few and stable ministries. Paper-based systems, and a "siloed" approach to information management, served as a primary way to protect personal information. The Ministry of Health had direct responsibility for the delivery of all health care and services, and control over the management and delivery of those services. Today, we have a very different model for achieving service requirements and outcomes: The Ministry of Health Services and its partner, the Ministry of Healthy Living and Sport, no longer deliver health services directly but fund and provide governance and oversight over many separate, but inter-related, health service organizations that deliver and manage health services.

The FOIPP Act has not "moved with the times", and is still predicated on an outdated model of information management in which each of these organizations, no matter what its mandate, operates as an independent public body. Each public body is assumed to be a separate "business" and required to independently protect the information in its custody or control, with no formal consideration as to whether it is related or even subsidiary to another. Under this model, each Health Authority has the responsibility and the discretion to determine what data they provide to the Ministry. In other words, the administrative (delivery) arm has the ability to choose what data to report to its oversight and funding body. This goes to the core of the current information stewardship problem, compromising the Ministry's ability to ensure effective accountability and stewardship of the health sector. Each of the many public bodies in the health system decides independently on data that was once available for common clients under a single Minister.

This model of many separate public bodies may reflect the health sector's administrative structure, but it does not support its service delivery or information management needs.

In dividing the Ministry of Health into the ministries of Health Services and Healthy Living and Sport, for example, the intention could not have been for the ministries to have to enter into service provider relationships or numerous and complex information sharing agreements with each other in order to be able to exchange needed data (especially when the ministries have shared responsibility for governance of the B.C. health sector); and yet, this is exactly the impact.

Example: Surgical Patient Registry *- In 1999, the Ministry established a surgical wait times website as a tool for patients and their physicians to help manage their surgical wait times (e.g., check to see how long the wait list is for surgeries; look at hospitals such as the Surgical Innovation Center where they might be able to schedule surgery with a lesser wait time; find a surgeon with a lesser wait list; and decide how best to proceed). One coordinating Health Authority was responsible for gathering individual-level data from operating room booking departments in all the other Health Authorities, and submitting it to the Ministry. The Ministry would then verify the data against acute (hospital) and vital statistics data to ensure data accuracy, and publish the surgical wait times in an anonymous format on its wait* time website.

In late 2009, the Health Authority coordinating the data collection advised the Ministry that it would no longer report required information in individual-level form because, in its view, individual-level data for the wait list did not meet the test for a "consistent purpose" under the FOIPP Act s. 33(a) because it was not "necessary" for wait list purposes. Although the Ministry does not agree with this interpretation, the decision with respect to disclosure was made by the Health Authority as a separate public body under the FOIPP Act.

Lack of individual-level information prevents the Ministry from ensuring that wait time data it publishes is accurate. Using only aggregated data means it is not possible to determine when a patient is on more than one wait list, or is wait-listed multiple times for multiple procedures. Surgeons and their patients cannot make informed decisions in this situation. The Ministry cannot accurately assess whether Health Authorities are meeting their wait list management obligations (e.g., not to wait list patients for more than one year). The Ministry also lacks the data to understand patients' health outcomes as they move from one level of service to another, and to determine if wait-time targets are met so millions of dollars of contingent funding can be released to Health Authorities.

Example: Home and Community Care minimum data reporting requirements (MRRs) - *MRRs were developed by the Ministry in consultation with Health Authorities as a primary funding and accountability mechanism to ensure that health authorities are meeting their service targets. They have been in place for a number of years. In 2009, however, one Health Authority refused to provide the Ministry with individual-level minimum reporting requirement data on the basis that it was not necessary or specifically authorized for the Ministry to have this data for a "consistent purpose" under s. 33(a) of the Act (even though FOIPP Act provisions had not changed nor had the data elements required). The same Health*

Authority advised that it was considering whether or not to stop providing the Ministry with hospital data for the same reason.

Challenge #2: *Artificial Barriers and Information Sharing Delays between Public Bodies*

Problem Description and FOIPP Act Challenge:

In the FOIPP Act today, "guaranteed" privacy protection hinges on each public body keeping its personal information away from other entities – including other public bodies. This regime fosters a "protectionist" rather than "cooperative" approach to FOIPP Act interpretation. The result is an unrealistically narrow interpretation of what information is considered "necessary" to steward the health system, and the misconception that all data can be used effectively at a statistical/aggregated rather than individual (personal) level. Health Authorities have argued, for example, that because the Ministry of Health Services does not provide individual care, it has no need to collect individual-level information.

Within the health sector, the sharing of individual-level data between public bodies has to be legally justified under the Act's rules for disclosure on one side, and collection on the other. Data exchange cannot take place without extensive negotiation, legal analysis, privacy impact assessments, security threat and risk assessments, information sharing agreements, and exhaustive justification for why the data exchange is required. As specific legal authority for the data exchange is preferred, the wording of any legal authority cited must be meticulously scrutinized, and if there is no explicit mention of the exact data exchange initiative, then there must be plans to put something in place. Documentation must be vetted by lawyers, regularly re-negotiated, and updated whenever any element of the data sharing arrangement is changed. One of the most common challenges within the health system is the length of time these documents require to negotiate and complete, particularly if multiple public bodies are involved. Delays are often compounded by lawyer to lawyer discussions designed to limit privacy risk and liability for each of the public bodies, even if the service goal is to partner in delivering health care.

The Ministry administers as many as 250 data access agreements in one year. Approximately one third of these agreements require complex information sharing provisions that can take from 6 to 18 months to negotiate at current staff levels, with an average of 8 months. In today's climate of fiscal restraint, the Ministry and Health Authority resources to manage these requirements are limited, and are competed for by increasing demands to monitor compliance with these same data access agreements. Delays and administrative barriers in collecting data compromise the ministries' ability to provide proper stewardship of the health sector. By the time the "information borders" between public bodies have been crossed, data is often out of date, or programs have been forced to move ahead without the data they need.

Example: "Divisions of Family Practice" initiative - I*n 2008, the Ministry of Health Services established a "Divisions of Family Practice" program to plan appropriate levels of after-hours care to relieve pressure on hospital emergency departments. Like so many other health issues, emergency room over-crowding is not an emergency department problem in itself, but is related to a number of factors,*

including lack of hospital capacity, lack of family practitioners, and insufficient clinic hours in the primary care setting. A provincial perspective was needed to analyze the flow of patients through different parts of the health sector. There was a need to look "upstream" and "downstream" from the emergency department area itself, and identify how family practices could help with management of emergency department wait times. Emergency department data from Health Authorities, combined with Ministry Medical Services Plan data, would help complete the picture of emergency care in the province and give the Ministry valuable information about how to reduce emergency room wait times. This was not an established program of the Ministry, but well within the ambit of the Ministry's health system stewardship role. However, it took nine months for the multiple participating Health Authorities to deal with the legal, privacy, policy and administrative processes required to bridge the FOIPP Act data sharing requirements between separate public bodies; it took two days to collect the data itself.

Challenge #3: *Restrictions on sharing of individual-level information for new initiatives*

Problem Description and FOIPP Act Challenge:

Innovative pilot programs and new initiatives are often circumscribed by FOIPP Act information disclosure (and corresponding information collection) restrictions. For instance, Health Authorities do not interpret s. 33.2(a), the "consistent purpose" provision, as permitting disclosure of data to the ministries for programs that do not fall within a "traditional" approach to health care, because the "new" use of the data would not have been contemplated at the time the information was collected. Section 33.2(d), which permits disclosure of data for "a common or integrated program" has been interpreted to require a formal relationship (i.e. a relationship established by a shared budget for the specific program, or explicit legislated mandate) to be established before information can be disclosed. Not surprisingly, most pilot programs and new initiatives do not enjoy explicit legislated authority or formally established program mandate, although they almost always involve collection, use and disclosure of data. This hampers timely responses to emerging issues, and the ability to implement new health service policy decisions in a timely manner. It also limits the scope for analyzing and sharing data to explore the potential for innovation, the viability of new programs, or the forging of new relationships.

Example: Early Childhood Vision and Dental Screening Program *- In 2005, the Premier announced a $73 million program to provide universal hearing, dental and vision screening for every child under age six. This initiative is led by the Ministry of Health Living and Sport, and forms part of a cross-ministry strategy to address dental, hearing and vision concerns in early childhood so as to limit their impact on children's development and learning. The Ministry of Health Services conducts data analysis for the Ministry of Health Living and Sport to assess the program's referral criteria and client screening tools. Individual-level data is needed so that it can be matched to Medical Services Plan data to evaluate the effectiveness of the vision and dental screening programs on children's health, and to determine whether children with key vision conditions (i.e., amblyopia, strabismus, refractive errors)*

are being identified. The data could also help to determine if referrals to eye doctors are being appropriately made, if screening referral criteria are appropriate, and what public health follow-up activities are associated with children's visits to an eye doctor following referral. Proper evaluation allows the program to avoid over or under-referrals (over-referral rates, for example, impact parents who must arrange time off to attend diagnostic appointments), correct and fine-tune referral criteria (so as not to miss children that need referrals), and find program efficiencies to conserve Health Authority resources.

The Health Authority involved in providing the care refused to give the Ministry of Health Services program assessment data because their lawyers were of the opinion that the FOIPP Act requires a formal "service relationship" between the Ministry of Health Services and the Ministry of Healthy Living and Sport before data can be shared between them. The Health Authority would not exercise its discretion to provide the data even when the Ministry obtained parental consent for indirect collection as required under s. 27 of the Act, because there was insufficient "paperwork" around the service relationship between the ministries. The inability to receive client screening data from one health authority compromises the provincial evaluation of dental and vision health screening programs and impacts provincial program planning.

Part of the Ministry's role is to give health service providers tools for managing health service delivery. The data that is collected in the course of developing, providing and evaluating these tools must in turn be available to the Ministry to evaluate their impacts and outcomes across the health system, for resource planning and quality assurance, and to devise new ways to manage citizens' evolving health care needs and expectations.

***Example: Integrated Health Networks initiative** - In 2008/2009, the Ministry piloted an "Integrated Health Networks" initiative. Interdisciplinary teams of practitioners, health authority and community resources were established with the specific objective of helping high-needs patients with multiple health conditions to manage their health. The Ministry established 26 distinct Integrated Health Networks across the province serving 50,000 patients in total. The goal was to keep these patients from becoming acutely ill, improve the experience of both providers and patients, improve outcomes, and reduce health system costs.*

Section 27 of the Act does not permit patient information to be collected from individual physicians (who are not public bodies) without either specific legislative authority or explicit consent. For pilot programs innovating in integrated service delivery such as this, specific legislative authority does not usually exist. The Ministry, Health Authorities, network teams, and participating physician offices had to establish a complex patient consent process. Patient consents were held by the health authority, but physician offices had to obtain them in the first place, and to maintain the consents as patients moved or their circumstances changed. In addition, because the teams shared clinical data between the Ministry, private practitioners and community resources, separate oaths of confidentiality were required for Health Authority staff to access patient files in physician offices – a

significant challenge within the employment and bargaining unit context. Managing this consent and confidentiality process delayed the project by almost a year, and cost 1 million dollars; and, due to the delay, the project also lost additional funding that might otherwise have been available.

Proposed Remedy:

Amend the FOIPP Act to recognize the "Health Sector"

If it is a priority to put government's limited resources to best use to ensure health system sustainability through proper management, accountability mechanisms, and evidence based decision making, then, from an information and data perspective, less segmentation between public bodies in a common sector would seem to make most sense. Given the network of different levels of organizations that make up and support integrated health services, it is time to introduce the concept of a broader "health sector" or "health family" of public bodies.

The Ministry of Health Services has responsibility for the overall management of a complex and changing health system. As such, it is logically the "parent" public body for the Health sector and has pre-eminent authority over the information necessary to manage the system. The Health Authorities play a key but subsidiary role in the health sector, in which they manage the delivery of services in partnership with the Ministry, each other, and with the constellation of bodies below them. They are more like "child" public bodies that exist by appointment of the Minister and must take direction from the Ministry but also manage their own responsibilities within those bounds. Within the family, information may be collected by one public body, but may also be shared and further used by other organizations in the health system. The Act should recognize the need for these bodies to interact in a cohesive way.

The definition of "health care body" already exists in Schedule 1 of the FOIPP Act, and could be amended to reflect this "health sector family" model. Alternatively, within the health sector public body system, the collection, use and disclosure of individual-level information could be authorized for health stewardship purposes (in a transparent manner and under direction of the Minister responsible) and as necessary for health service programs, following established codes and best practices. Individual-level data could not be used indiscriminately throughout the Health System, as there are over twenty pieces of health legislation that govern health programs and their information, including the *E-Health (Personal Health Information Access and Protection of Privacy) Act,* which would continue to operate alongside even a modified legislative framework.

Concluding Comments

"Opening the borders" to information sharing will improve the ministries ability to provide the effective stewardship of the health system that translates directly into reduced wait times for surgery, shorter emergency room wait times, more available hospital beds, longer clinic hours, and better tools for managing diabetes, asthma and other health conditions.

Almost two decades of experience with the FOIPP Act have resulted in a well-developed access component. It is time now to modernize the protection of privacy component, which reflects a bygone era of government structures and information media. This

modernization must equip government to be agile in responding to and utilizing advances in information technology, evolution in government service delivery, and associated higher public expectations around data use and analysis for service planning, management and health sector stewardship.

Appendix – Description of Ministry Mandates

Ministry of Health Services

The Ministry of Health Services has overall responsibility for ensuring that quality, appropriate and timely health services are available to all British Columbians. The Ministry performs this leadership role through the development of social policy, legislation and professional regulation, through funding decisions and fiscal management, and through its accountability framework for health authorities and oversight of health professional regulatory bodies.

Through the ministry, the Province funds health authorities as the organizations primarily responsible for health service delivery. Five regional health authorities deliver a full continuum of health services to meet the needs of the population within their respective geographic regions. A sixth health authority, the Provincial Health Services Authority, is responsible for managing the delivery, coordination and accessibility of selected province-wide health programs and services. The Ministry works with health authorities, care providers, agencies and other groups to ensure the provision of universal access to health care. The Ministry provides leadership, direction and support to these service delivery partners and sets province-wide strategies, goals, standards and expectations for health service delivery by health authorities.

Ministry of Health Living and Sport

The Ministry of Healthy Living and Sport was created to help British Columbians lead healthier lives and make choices for themselves and their families that make a real difference in their ability to remain healthy, active and enjoy life to its fullest both now and in the future. The Ministry supports Government's Great Goal #2: *Lead the way in North America in healthy living and physical fitness* and provides a foundation for healthy living by focussing on improved air, water, nutrition, physical activity, and vulnerable populations. The Ministry works to enhance the focus and integration of public health programs, services and information by supporting a strengthened and renewed public health system and increasing long term sustainability of the health care system.

The Ministry's core business areas are Population and Public Health; Provincial Health Officer; Sport, Recreation and ActNow BC; and the B.C. Olympic and Paralympics Winter Games Secretariat. The Ministry of Health Services works collaboratively with the Ministry of Healthy Living and Sport to guide and enhance the Province's health services to ensure British Columbians are supported in their efforts to maintain and improve their health.

The Ministry of Healthy Living and Sport is also responsible for the following legislation: *New Public Health Act*, *Food Safety Act*, *Community Care and Assisted Living Act*, *Drinking Water Act*, and the *Tobacco Control Act*.

CITIZENS' SERVICES

Ministry Mandate

The mandate of the Ministry of Citizens' Services (MCS) is to transform, deliver and promote services that are cost-effective, accessible and responsive to the needs of citizens, businesses and the public sector.

MCS provides front-line services to citizens on behalf of other ministries, and also provides much of the enabling infrastructure and services that government needs to perform core business operations efficiently and effectively. MCS is also leading the advancement of innovation and collaboration across government. Through this role, the ministry is responsible for modernizing the internal operations of government and developing the strategies to ensure an engaged workforce is able to meet the demands of the future.

MCS brings the centres of expertise for the strategy, planning and support of public service delivery under the umbrella of a single ministry with a clear mandate to transform how citizens interact with their government. Four defined areas of responsibility are linked under the umbrella of MCS:

1. MCS sets the direction to enable effective and innovative citizen-centred services.
2. Shared Services BC integrates the delivery of goods and services to provide innovative, responsive and cost-effective services to the public sector. Shared Services BC supports government as the lead agency for procuring and supplying the technology, accommodation, products and services required by government and the broader public sector to provide services to the people of British Columbia.
3. The Public Service Agency provides human resource leadership, expertise, services and programs that contribute to better business performance of ministries and government as a whole.
4. The Public Affairs Bureau leads and co-ordinates communications with internal and external stakeholders, ensuring that citizens are informed about government policies, programs and services, and that information is communicated in an open and transparent manner.

A key focus of MCS is on the continuous improvement of the quality of services and pursuing innovative business solutions that meet the changing needs of citizens, customers and clients by strategically aligning the business, technological and human resources of government.

Better Outcomes

Challenge #1: *Information Sharing in Common and Integrated Programs and Activities*

Problem Description:

MCS is responsible for providing advice and assistance to the development of corporate initiatives (involving more than one ministry and or public body or having major implications for government) related to information sharing and privacy.

Within the last 12 to 18 months, MCS has worked with several ministries on the design and implementation of common or integrated programs, including the Ministries of Attorney General, Housing and Social Development, Children and Family Development and Public Safety and Solicitor General. A number of these projects are discussed in further detail in this report.

Passed in 2005, the common and integrated program or activity disclosure provision (s. 33.2(d)) was intended to promote information sharing across ministries and government agencies to support provision of a common service, program or activity to a common group of clients. It was added as an explicit recognition of the move across government to provide horizontal and integrated services to meet the needs of citizens and provide more programs in a more coordinated and effective way.

The reality is, however, that there are problems applying this provision in practice that act as barriers to the effective design, development and implementation of common or integrated programs or activities. In assisting ministries in working through the privacy and information sharing requirements related to a common or integrated program or activity, MCS has been made aware of the various challenges and impediments within the FOIPP Act related to inconsistencies and gaps in the collection, use and disclosure provisions that impede the effective implementation of common or integrated programs or activities. Many of these same issues are highlighted and discussed in Ministry sections.

FOIPP Act Challenges:

- The collection provision creates interpretation challenges when coupled with the disclosure provision for the purpose of delivering a common or integrated program or activity. The current authority for collection that is most applicable to the delivery of a common or integrated program or activity requires that collection ". . . ***relates directly to and is necessary*** *for an operating program or activity of the public body*". The clause, "relates directly to and is necessary for an operating program or activity of the public body", creates interpretation challenges with regard to collecting information in the delivery of a common or integrated program or activity. When multiple public bodies participate in a common or integrated program they may need to collect information necessary and related to the delivery of the joint program that may not always be necessary and related to their specific organization.

- The use of the word *"the"* in the collection provision - *"relates directly to and is necessary for an operating program or activity of the public body"* – creates further challenges as it implies a standalone public body approach which has been interpreted by some public bodies as such, preventing a common or integrated approach.

- The language and sentence structure used in disclosure s. 33.2(d) does not fully support a common or integrated program or activity approach. The specific reference in s. 33.2(d) includes a requirement that information must be necessary "*for the performance of the duties of the officer, employee or minister to whom the information is disclosed*". Common or integrated programs or activities are comprised of several public bodies and other agencies. In order for such initiatives to work, one public body needs to be able to disclose to all public bodies participating appropriate information to ensure the successful delivery of the common or integrated service. This means that some information may not be necessary for the duties of every representative participating in the program during every information exchange but is needed for the overall delivery of the common or integrated program or activity. While it is recognized that representatives use discretion when disclosing information, if each public body participating disclosed information only a case-by-case basis to each representative separately, then the concept of common or integrated program is meaningless.

  Example - *Daniel has recently appeared before the Vancouver Community Court (VCC). The VCC is an integrated program where participants work collaboratively to identify offenders' needs and circumstances and develop recommendations for interventions for consideration by the court. Following the court's determination, the team comes together again to develop a case management plan consistent with the court's direction and drawing on previously developed recommendations.*

  The case management plan for Daniel includes solidifying housing and social assistance support. Daniel receives housing support by way of placement at a shelter and while the immediate housing challenge for Daniel has been resolved, the housing representative continues to attend VCC meetings related to this individual. At the last meeting, it was learned that Daniel is now receiving income assistance. This means that Daniel can leave his shelter placement and with financial support now established his living arrangements can be improved, including locating his housing in the same area where he attends community programming. If the housing and income assistance representative had not been able to continue to work with the others and learn of Daniel's improved income and where he was attending community programming, because it could be argued that that information being disclosed to the housing representative was not necessary for the performance of their duties, they would not have been able to further assist and help stabilize Daniel in the community.

- The disclosure provision that allows the delivery of a common or integrated program or activity has the effect that only public bodies can participate in such a program or activity. The FOIPP Act limits the agencies that can participate in the

delivery of a common or integrated program or activity by specifying that disclosure can only occur within a common or integrated program or activity to "an officer of employee of a public body".

Public bodies as defined by the FOIPP Act are ministries, health authorities, municipal police, municipalities, school boards, colleges and universities, crown corporations, self-governing professions and other bodies. However, a public body is not a federal government body (such as the RCMP) nor is it an agency of another provincial government (e.g. Yukon Health and Social Services) or a community agency (such as a not for profit program). The B.C. Government requires interaction with other jurisdictions and community agencies in the delivery of some integrated services to citizens to ensure a fulsome response to the challenges that citizens may face and the services they receive.

> ***Example*** *- An integrated program operating in Victoria includes Vancouver Island Health Authority, the Ministries of Public Safety and Solicitor General, Housing and Social Development and the Victoria Police. The program wants to expand and serve Colwood and Langford. However, these areas are served by the RCMP who are not defined within the FOIPP Act as a public body, therefore, difficulties arise in achieving the program expansion.*

Proposed Remedy:

Revise the FOIPP Act to provide for effective and comprehensive approach to common or integrated programs or activities, including:

- Enabling the collection of personal information by public bodies participating that is necessary and related to the delivery of the joint program but may not always be necessary and related to their specific organization;
- Allowing provincial public bodies to share personal information with non-public bodies for the purpose of delivering a common or integrated program including, other provincial and federal public bodies and community agencies as appropriate.

Benefits to Citizens:

Amendments to the common or integrated program or activity provision to clarify collection and disclosure by and among public bodies and other parties necessary to the program delivery ensures a fully functional and integrated approach for citizens. Citizens are better supported when multiple agencies participating in a common or integrated program or activity function as one rather than trying to continue to provide support services in a siloed way. Additionally, delivering services through common or integrated programs or activities ensures services to citizens are not limited by various levels of governments or by provincial or community borders.

Challenge #2: *Definition of Law Enforcement*

Problem Description and FOIPP Act Challenge:

To further support the common or integrated program or activity, particularly in the social and justice sectors, the definition of "law enforcement" under the FOIPP Act should be reconsidered. The Criminal Justice Reform Secretariat reports that much of an offender's behaviour can be linked to substance abuse and additions, mental

disorders, lack of job skills and other issues and not just criminal activity. The secretariat further reports that evidence shows that referring offenders to the services they need, and coordinating programs both social services and enforcement, has broad benefits for communities by reducing crime rates and chronic criminal behaviour.

The FOIPP Act defines "law enforcement" to mean:

a) policing, including criminal intelligence operations,

b) investigations that lead or could lead to a penalty or sanction being imposed, or

c) proceedings that lead or could lead to a penalty or sanction being imposed.

Based on this definition, public bodies interpreting the legislation define policing differently but generally most interpret it to only mean the enforcement of laws and not the prevention of crime or other policing responsibilities such as those referenced in British Columbia's *Police Act*, s. 7:

> "The provincial police force, under the commissioner's direction, must perform the duties and functions respecting the preservation of peace, the prevention of crime and offences against the law and the administration of justice assigned to it or generally to peace officers by the commissioner, under the regulations or under any Act."

B.C.'s *Police Act* includes language that clearly notes that duties and functions of the province's police force include the prevention of crime and the preservation of peace.

Proposed Remedy:
Expand the definition of law enforcement in the FOIPP Act to reflect broader language contained in the Province's *Police Act* around crime prevention and preservation of peace.

Benefit to Citizens:
Aids in the rehabilitation of offenders as well as improves safety in communities by enabling the ability to collect and disclose personal information when and as appropriate, if there is an identified need related to preventing crime and keeping the peace.

Challenge #3: *Limitations on Program Evaluation*

Problem Description and FOIPP Act Challenge:
Program planning and evaluation is an important component of service delivery. Citizens in receipt of services need to be confident that the services they receive are well planned and appropriately reviewed to ensure they meet their specific needs. As taxpayers, they also need to know that the services offered by government represent value for money. Citizens cannot make informed decisions about whether a government program meets their needs or produces the expected outcomes unless government is able to evaluate the effectiveness of programs offered and provide this information to citizens.

The FOIPP Act does not include explicit legal authority for public bodies to disclose personal information for the purpose of program planning and evaluation that will help to ensure services to citizens are effective.

The FOIPP Act, s. 35 allows public bodies to disclose personal information for the purpose of research: a "public body may disclose personal information or may cause personal information in its custody or under its control to be disclosed for a research purpose, including statistical research ...". However, the term research is not defined in the FOIPP Act and has been interpreted by some public bodies as relating only to scientific research, where an assumption is analyzed and reviewed. This interpretation does not accommodate initiatives that require applied research into facts and trends and service delivery approaches, which can provide valuable information toward program evaluation and/or planning and where the intention is not to use personal information to make decisions about specific individuals but to determine if the services received by citizens are appropriate and effective. Performance evaluation provides evidence as to whether or not multiple services received by citizens are complementary and beneficial or if they overlap or leave service gaps. This type of evaluation also helps to determine if citizens are receiving value for money.

> ***Example -*** *John has been homeless for a number of years. His living situation coupled with his mental illness and addiction, designates him as a chronically homeless individual. He receives supports from a number of ministries, government and community agencies. He also frequently attends the hospital emergency rooms and engages in conflict with the police. Agencies and ministries want to develop ways to better support chronically homeless individuals like John, rather than the existing disparate approach.*
>
> *For a complete picture of the services John and other homeless people receive including identifying gaps and overlaps, information must be collected from the agencies and ministries providing services. Some agencies do not want to provide the information because, while the FOIPP Act enables the sharing of personal information for research purposes, agencies refuse because they do not believe that the definition of research includes determining service levels and, the effectiveness of programs overall and as delivered by separate public bodies.*

Proposed Remedy:

Modify language in the FOIPP Act so that it is interpreted in its grammatical and ordinary sense, to ensure a broader approach to research including under s. 35 applied research into issues, facts, trends, etc. for the purpose of program planning and/or evaluation.

Benefit to Citizens:

Citizens, as clients and taxpayers, receive optimum services through well-planned program delivery and as program effectiveness will be evaluated, citizens are also able to determine if a program or service is able to meet their individual needs.

Citizen Centred Service

Challenge #4: *No Authority to Collect a Citizen's Personal Information with Their Consent*

Problem Description:
Currently citizens cannot provide government ministries and agencies permission to collect their personal information to achieve such things as providing better citizen supports because there is no specific authority contained in the FOIPP Act. Unlike, private sector personal privacy legislation, the FOIPP Act does not provide the ability to collect personal information on the basis of consent by an individual.

FOIPP Act Challenges:
Under the FOIPP Act collection (s. 26) is limited to:

a) the collection of that information is expressly authorized under an Act,

b) that information is collected for the purposes of law enforcement, or

c) that information relates directly to and is necessary for an operating program or activity of the public body."

The restrictive nature of these three requirements coupled with a definition of 'public body' that divides government by ministries and agencies creates impediments to providing citizen centred service delivery. This coupled with s. 26(c) (above) which provides collection authority in support of program and service delivery but which also stipulates that the personal information must relate directly to or be necessary for the public body, impedes service delivery for citizens.

For example, an individual cannot provide a government organization, such as Service BC, that delivers in-person services on behalf of the provincial government in 60 communities throughout British Columbia, with consent to collect information on behalf of other government agencies. A grieving citizen who visits a Service BC Office requesting support to ensure proper documentation is completed relative to the death of their spouse cannot ask Service BC to facilitate this on their behalf. Instead they are required to attend or contact various provincial and federal offices to cancel such things as drivers' licences, advise Revenue Canada of the death of their spouse and ensure they have their own health benefits accounts.

Proposed Remedy:
An individual's consent to collection of their personal information should be included in the FOIPP Act. The revised provision should be aligned with the consent provisions as provided in the *Personal Information Protection Act* (PIPA), s. 6 that allows an individual to consent to the collection, use or disclosure of their personal information.

Benefits to Citizens:
Citizens can authorize the collection of their personal information by one public body on behalf of another public body or government agency, creating efficiencies for citizens as they interact with the province and various levels of government.

Challenge #5: *The FOIPP Act is Not Consent-Based*

Problem Description and FOIPP Act Challenge:
The FOIPP Act is not considered to be consent-based legislation and therefore does not contain a framework that permits government to collect, use and disclose personal information based on various kinds of consent except in the case of use and disclosure where explicit written consent is a legitimate authority. This is very different from private sector privacy laws, where implied consent is a legitimate basis for collecting, using and disclosing an individual's personal information if a reasonable person would interpret the individual's actions as authorizing such activities. For example, if a person pays for tickets online for a sporting event, it is implied by this action that the individual has authorized the ticket agency to collect, use and disclose the individual's personal information for the purpose of obtaining the payment and sending the tickets to the payee.

As a result of the provisions of the FOIPP Act, government is unable to assume from an individual's actions that they have consented to their information being collected, used or disclosed. Often this is contrary to the public's expectation.

Proposed Remedy:
The FOIPP Act should be amended to allow similar considerations as are included in PIPA, s. 8 (implicit consent) which deems consent to the collection, use or disclosure of personal information for a purpose if, at the time the consent is deemed to be given, the purpose would be considered to be obvious to a reasonable person and the individual voluntarily provides the personal information for that purpose.

Benefits to Citizens:
Citizens will be able to purchase or enroll in services online as they would in the private sector and assume that the information they have provided for payment and provision of services will be sufficient, without them having to fill in additional forms or agreements. This will simplify the online experience for citizens.

Stronger Engagement

Challenge #6: *Limitations on the Use of Technology to Engage Citizens*

Problem Description:
Citizens want their government to be available to them in as many ways possible. They want to voice their opinions on the management of their province, including the laws that govern them, the services offered to them and the policies and practices of the employees that serve them. To effectively engage citizens, governments must keep pace with an evolving world. This means providing citizens with the ability to communicate with government in the most current and convenient ways available. When governments make themselves available in a variety of ways by establishing a number of different communication methods, they place themselves in the best position possible to ensure they are able to be fully engaged and listen and consider as many citizens' views as possible.

The FOIPP Act presents challenges to government with regard to citizen engagement and the use of new and evolving technology including social media and the internet. As noted, the FOIPP Act was written in 1992 when the internet, social networking and other technological advancements were either not developed or as utilized as they are today and where current operation and business needs of government, using new media and information technologies to provide effective service and better engage citizens, was not contemplated. While in some cases government has developed remedial solutions, these solutions are administratively burdensome.

FOIPP Act Challenges:

The FOIPP Act creates barriers where there is no reasonable expectation of privacy on the part of a participant using social media and other technology by placing geographical restrictions on government that contribute to limited sharing.

The FOIPP Act enables a public body to disclose personal information inside or outside Canada under a number of circumstances; however, absent explicit consent, or a ministerial order, the Act does not provide for disclosure outside of Canada when an individual is voluntarily participating in and knowingly posting to a public domain. Social networking sites are housed outside of Canada, so when the government creates a presence within a social networking site, and citizens post comments or opinions, or use identifiers such as email addresses, which are defined as personal information under the FOIPP Act, it could be that by having a presence in a site outside of Canada and hosting citizens' personal information there, government is disclosing personal information outside of Canada. Citizens posting information are doing so knowing that the information is in the public domain, so there is no expectation of privacy. Additionally, government is constrained if it wants to respond to a question posted on a social network site. By simply placing the individual's name in the salutation and posting that to the site, government is disclosing personal information outside of Canada.

Social media is an important communication tool for governments and citizens. The BBC reports that social media could transform public services[7] and claims that since it has "happened to the music and travel industries" it is also "going to happen to public services". Canadians are particularly active in social networking according to a recent Vancouver Sun article which notes that, "social media is cutting across all generations" and that, "four out of five online Canadians use social media"; more than Americans and those in the United Kingdom[8]. With the existing FOIPP Act barriers, government's ability to communicate with British Columbians using mainstream technological and communication tools is hampered by legislation that, when written, did not contemplate such technology.

[7] Social media 'could transform public services" BBC News November 27, 2009

[8] "Canadians tops in social networking" Vancouver Sun, December 03, 2009.

The other challenge with the FOIPP Act relates to the disclosure of personal information through the internet. When government posts personal information to the internet it is disclosing information outside of Canada, because the information can be accessed in other countries. Personal information for the most part is safeguarded from internet display; however there are instances when government identifies a need to post such information. For example, stakeholders would like government to routinely release information about government practices and compliance outcomes and to make that information easily accessible. In order to maximize distribution of the information to as many citizens as possible government would like to post it to the internet. In these instances, there are many companies and individuals who interact with government and it can be difficult for government to determine which licences or compliance records relate to companies and are therefore not personal information and which relate to individuals interacting with government in a personal capacity. Under the current disclosure provisions in the FOIPP Act, and absent a ministerial order, government would need to evaluate each list and each name to determine whether personal information is contained in the list before it could post it to the internet. This type of 'check' would be very time-consuming and involve the evaluation of multiple records, potentially researching numerous names and making telephone calls as necessary to verify the individual's role (e.g. personal or business). As a result, information that the public would like to see routinely available is often not posted publicly due to outdated restrictions in the FOIPP Act. While government could put some of the information out publicly in a reading room at a local office, this method of distribution is limited as individuals in rural areas, or those who are disabled or lack transportation, are unable to readily gain access to the information. Posting the information on the internet permits broader distribution and equal access for all.

Within the current FOIPP Act, there are two sections that could support disclosure outside of Canada. However, these sections also pose administratively burdensome and cumbersome workarounds for government and citizens.

The first section that can enable disclosure is s. 33.1(1)(b) which states that a public body may disclose personal information referred to in s. 33 inside or outside Canada if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure. So while this section enables disclosure by consent, it places barriers to the ease and use of social networking sites for citizens and for posting information to the internet. In order to become operational, this section requires that citizens consent prior to using a government social networking site. This means that if a citizen is using a site, they would have to agree to the terms and conditions of using the site and then provide consent either once they reach the government's site or when they post information or have an exchange with government, even when they know their actions, such as posting an opinion, are being done in a public domain. This is a process citizens do not have to complete when using other public or government sites. These supplementary steps are cumbersome to citizens and would very likely decrease the number of citizens engaging government through social networking tools. Additionally and with regard to the internet, when there is minimal personal information to be posted and a minimal number of individuals to contact, obtaining consent is not difficult. However, in the case of the example cited above (that is, culling through lists of names to identify which meet the definition of

personal information), it would only add to the already heavy processes government would need to undertake to post records.

The second section that could be used within the FOIPP Act is s. 33.1(3) that allows the minister responsible for the FOIPP Act, by order, to allow disclosure outside Canada in specific cases or specified circumstances, where the disclosure is authorized within Canada. The sections within the FOIPP Act that allows disclosure outside of Canada are so limited and prescriptive that government can only undertake disclosure of personal information either through the internet or a social networking site through a ministerial order. To make such an order in every instance in which legislation is deficient to allow disclosure outside of Canada, is a cumbersome and awkward way to manage government business.

Proposed Remedy:
The FOIPP Act should be amended to allow disclosure outside Canada for the purpose of engaging citizens through the use of mainstream technology that is not located in Canada when an individual is voluntarily participating and knowingly posting to a public domain. Additionally, the FOIPP Act should be amended to allow personal information to be disclosed outside of Canada in circumstances that does not hinder government's ability to share appropriate personal information with citizens such as noted in the example above; posting a list to the internet. Any amendments with regard to disclosure outside of Canada should to the greatest extent possible consider the evolution of technology.

Benefits to Citizens:
Allows government to provide citizens with more information and allows citizens to interact with government using mainstream technology.

Challenge #7: *Determining when Personal Information is Collected*

Problem Description and FOIPP Act Challenge:
Every day government ministries and other public body agencies receive large volumes of information from the public. In some instances, the information has been requested, as when government seeks input on a particular topic or when individuals submit information (personal and non-personal) that is required to receive a benefit from government. In other instances, the information has not been directly sought or required but relates to the mandate of the ministries or agencies. For example, an individual may submit a complaint about the way a program is run or the implications or consequences of the legislation the ministry's operations are based on.

In still other cases, the information that is sent to government does not have any bearing on the mandate or operations of the ministries or agencies that receive it. For example, the Ministry of Agriculture may receive an excellently compiled package of material containing many international articles on the topic of crop circles. While the information may have merit it might not be something that the Ministry of Agriculture needs to administer its programs. If the material does not contain personal information the ministry can manage it according to standard records management practices. If the information is of a personal nature, and meets the definition of personal information

under the FOIPP Act, the ministry is only permitted to collect it as authorized under the FOIPP Act (see below).

The concept of collection of personal information is an important one in the FOIPP Act, and to date there has been little in the way of jurisprudence delineating exactly when collection takes place. If information is considered to be collected as soon as it reaches government, by hard copy, or when it is posted in an electronic environment, an issue arises under the FOIPP Act as government could be operating in contravention of the collection requirements which are that the collection of the information must be authorized under statute, is for law enforcement purposes or relates directly to and is necessary for an operating program or activity of the public body.

Currently, government operates on the principle that there must be a decision made by a ministry that it wishes to collect personal information for it to be considered to be collected under the FOIPP Act. This means that personal information cannot be "volunteered" to a ministry and once received it is deemed to have been collected. For example, when a resume arrives at a ministry office through whatever medium, if it is unwanted and simply shredded, it is considered "received" but not "collected" (the term used in the FOIPP Act), as there was no intent for the ministry to collect the information. On the other hand, if the ministry decides to file the resume in case there is a future vacancy, there has been a decision to collect that information, and therefore the resume has been collected. Difficulties in this regard also occur within the context of social media where two points for collection arise. If a ministry solicits information from users, for example by way of asking a question, a collection occurs by the ministry of that solicited information when it is saved to the social media site. In terms of information that is not solicited (an individual posts an opinion to a site where opinions have not been sought) collection only happens once a ministry employee decides to save or print the information from the site.

If this interpretation of when collection occurs is not accurate, then government will have a much larger volume of information from the public to process, maintain, protect and otherwise manage in accordance with the requirements of the FOIPP Act. Some of this information will also be collected in contravention of the collection requirements of the FOIPP Act. In addition, a different assessment of the point of collection will severely impact government's ability to utilize social media sites as government cannot control what is posted to a social media site and if it is considered to have collected whatever information that is posted at the time it is posted, then it would be operating outside of the FOIPP Act for personal information that was not related to or necessary for its programs or activities.

> ***Example -*** *The Ministry of Environment could use social media, specifically Facebook to solicit ideas for revisions to the Water Act. If the point of collection for personal information is confirmed to be the same as that currently being used by government, the ministry would be able to save and/or print off information that was responsive to the questions that it had posed on its social media page and ignore that which was nonresponsive, unnecessary and unrelated to the mandate of the ministry. It would not be offside the collection provisions of the FOIPP Act. If, however, the point of collection is deemed to be different than what is currently*

practiced, the ministry could be operating in contravention of the FOIPP Act as the public may (and is most likely to in some instances) post personal information to the site that is unrelated to or tangential to the topic under discussion. The person posting may enter their own or others experiences on the topic of water or other issues or may go into great details about another individuals perceived misuse of this valuable resource. If this personal information is not related to or necessary for an operating program of the ministry, or authorized under an enactment or for the purpose of law enforcement, the ministry is in contravention of the FOIPP Act simply because a member of the public has posted something to the ministry Facebook site that the ministry neither wanted to needed.

Proposed Remedy:
Revise the collection provisions of the FOIPP Act to clearly state the point at which collection of personal information occurs. Ideally, this would be at the point at which a public body has decided to save, print, use or make a decision to retain the information that has been provided to it.

Benefits to Citizens:
Will solidify for citizens how and when government collects, and becomes responsible for, the management of citizens' personal information.

Challenge #8: *Storage of Personal Information in Canada, Subject to Exceptions*

Problem Description and FOIPP Act Challenge:
Section 30.1 requires a public body to ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada unless the individual the information is about has identified and consented; unless it has been disclosed for a purpose defined within the FOIPP Act (for example in accordance with an enactment of British Columbia or Canada that authorizes or requires its disclosure); or if it is disclosed to allow the collection of amounts owing to government or a public body.

The application of these sections limits government's ability to evolve with regard to the internet and the services provided through it. Some of these limitations and impacts include constraining the use of technology and technology services, negatively impacting government's competitive edge and not allowing service delivery changes to occur.

For example and as mentioned previously, social networking sites are housed outside of Canada. When government creates a presence within a social networking site, and citizens post comments, opinions or use identifiers such as an email addresses, which are defined as personal information under the FOIPP Act, government is in effect, by having a presence in a site outside of Canada and hosting citizens' personal information on it, storing personal information outside of Canada.

Additional initiatives constrained by s. 30.1 relate to future models of information technology, which move away from traditional models currently used by government to new technologies and services where information technology services are offered or

presented over the internet. This type of information technology service delivery is referred to as 'cloud computing'.

The traditional information technology service delivery model established today relies on local deployment of computing infrastructure usually committed to government, in particular the servers in which information databases and applications reside. Today's service delivery model requires physical locations to store servers, expert resources to manage the infrastructure, and customized software to meet government's needs either for government staff for use in their day to day work or for citizens accessing information and services from government.

Enabling storage outside Canada, in certain circumstances with established safeguards, would ensure that government remains relevant to the online world as it could draw on commonalities of hosted services over the internet which means government could:

- offer the same services and service features that are as technologically advanced as those that are used and expected by citizens and the private sector,
- host and provide information services to citizens and its workforce through more cost effective means, and
- maintain its competitive edge.

One provision related to storage outside of Canada that may enable government to operate fully either with regard to social media or cloud computing is the consent provision. However, because this provision is so prescriptive, in that it only allows storage if the individual has identified it and consented in the prescribed manner, it makes the provision unworkable. For example, if there is an email exchange about scheduling an interview for an individual and the individual's resume, which is personal information, is attached to that email the individual would have to consent to the storage of the email. If government had to continuously undertake these steps, the situation would become unmanageable. Additionally and with regard to the difficulties with consent and social media, as mentioned previously the steps citizens would need to take in order to participate in a government social networking site will present a cumbersome process for citizens and deter use.

> ***Example -*** *Grade 12 students across B.C. are participating in a forum with other students from England, New Zealand, Japan and Australia learning about the perception of world events from the perspective of different cultures and traditions. Students participate in a virtual classroom using the "Second Life" game environment. Papers, presentations and work group projects are created and accessed using Google tools which offer compatible resources for all participating students regardless of their physical location. Working within the virtual world using cloud computing resources allows students from across the world to learn from peers in other countries in an environment that is relevant to their interests. It also removes barriers for families who are unable to afford travel for their children, as students regardless of their family's economic situation, are able to learn firsthand about other countries, traditions and culture.*

Proposed Remedy:
Amend the provision to allow storage outside of Canada in specified circumstances while ensuring personal information is appropriately safeguarded.

Benefits to Citizens:
Citizens, as clients and taxpayers, are assured that services are provided in a way that offers current technological advances through the most cost effective means while ensuring appropriate safeguards and spending. While there has been concern regarding the United States government accessing information about British Columbians under the *USA Patriot Act*, government would work to develop appropriate and adequate measures to protect information. The extent of these measures would be dependent on the type and sensitivity of the information and the context (e.g. social networking site voluntary participation).

CONCLUSIONS AND RECOMMENDATIONS FOR AMENDMENTS TO THE FOIPP ACT

Observations and Conclusions

The nature of the way government does its work and delivers programs and services to citizens has changed significantly over the past 15 years. Government ministries, and other public bodies, are encountering common difficulties and challenges with the FOIPP Act in attempting to implement innovative new ways of providing services to provide more effective, integrated and coordinated programs and meet citizen's needs and expectations. In many cases they have adapted, accommodated and adjusted programs and approaches to mitigate impediments to information sharing. In some cases these adjustments result in less efficient and effective service delivery. In other cases, current privacy protection provisions in the legislation prevent integrated and innovative new programs or service delivery models from being implemented. Of particular concern are the provisions limiting the ability to collect and share information even with consent of the individual or under necessary circumstances and the provisions preventing the sharing of information among a range of partners in the delivery or a common or integrated program or to deliver service or programs for a common purpose benefiting the citizen.

Amendments to the FOIPP Act are recommended to address these issues, to facilitate government implementing new approaches to provide enhanced services to citizens and to allow government to leverage opportunities presented by technological advances to provide more efficient, timely and accessible service to meet citizens needs and expectations.

Summary of Recommendations for Amendment to the FOIPP Act

Following is a summary of common recommendations for amendment to the FOIPP Act that appear in multiple places in the submissions:

Consent, Collection and Disclosure

- Amend the consent provisions to allow an individual to consent to the collection, use or disclosure of their personal information by a public body (similar to PIPA).
- Amend the FOIPP Act to allow for indirect collection by, and disclosure to and between all relevant public bodies, without consent, for purposes of integrated program or activity; where of benefit to the citizen and necessary to the delivery of the service or program; and/or for public health and safety.
- Amend the FOIPP Act to allow for indirect collection by, and disclosure to, non public bodies (RCMP, NGOs and social service providers, government and police agencies in other jurisdictions), without consent, for the purposes of integrated programs or activities; where of benefit to the citizen and necessary to the delivery of the service or program and/or for public health and safety.
- Amend the FOIPP Act to provide for implicit consent (similar to PIPA).

Consistent Purpose

- Amend the consistent purpose provisions to ensure the full, comprehensive and effective application of this provision as the basis for information sharing, including that consistent purpose covers information sharing (collection and disclosure) within the public body and between all public bodies where the sharing supports the provision of the program or service, and related services, to the citizen, meets the citizens' service needs and provide seamless, integrated program and service delivery (including integrated or common programs or activities addressing domestic violence, homelessness and integrated justice or crime reduction programs).

Common or Integrated Program or Activity

- Amend the FOIPP Act to facilitate delivery of integrated programs by ensuring full and effective information sharing under common or integrated programs and activities (i.e., integrated or common programs or activities addressing domestic violence, homelessness and integrated justice or crime reduction programs) including:
    - recognizing the range and scope of potential common or integrated programs or activities to meet and serve the needs of citizens (not limited to programs or activities with structural arrangements, but rather based on delivery of a common or integrated function);
    - allowing for the collection and disclosure of personal information, both indirect and direct, within common or integrated programs or activities among all relevant parties, including public bodies and non public bodies (RCMP, NGOs and social service providers, government and police agencies in other jurisdictions); and
    - streamlining and providing for the appropriate records management requirements to enable effective and efficient information sharing in a common or integrated program while ensuring the security and protection of personal information.

Storage of Personal Information Outside of Canada

- Amend the provisions in the FOIPP Act prohibiting the storage of information outside of Canada to take into account IT developments and advancements that make jurisdictional boundaries artificial, including social networking and other internet tools and mechanisms that can promote stronger citizen engagement and to take advantage of commercial and economic opportunities for storage and management of information including "cloud computing".

Research and Evaluation

- Amend the FOIPP Act to include language confirming a broader approach to research so that applied research into issues, facts, trends, etc. for the purpose of program planning and/or evaluation can be undertaken.

Other Recommendations

Following is a list of specific recommendations made by individual ministries:

Ministries of Attorney General and Public Safety and Solicitor General

- *Definition of law enforcement* - amend the FOIPP Act to broaden the definition of "law enforcement" to include crime prevention or reduction programs and provide that information may be collected for these purposes;
- *B.C. Corrections Security Systems* - amend the FOIPP Act to clearly recognize that the protection of custody setting security footage is integral to effective law enforcement and add an explicit reference in s. 15(1) that authorizes a public body to refuse to disclose information to an applicant that could reasonably harm the effectiveness of custody setting security systems;
- *Police Audits and Other Oversight Functions* - Amend the FOIPP Act to strengthen the protection of privacy of personal information in police audits and other oversight functions by exempting any records generated from *Police Act* audits and examinations from the access provisions of the FOIPP Act;
- *Timelines for Public Reports* – amend the FOIPP Act to provide more appropriate timelines for compiling a major report for publication;
- *Courts Records* – amend the FOIPP Act to change the term "record in a court file" to "court record" and include a current definition of "court record" that takes into account new technology such as "Court Services On-Line" that provides greater access by the public to court record information.

Ministry of Housing and Social Development

- *Personal Information* – Change the definition of "personal information" to "private information" in recognition that the not all personal information is private and sensitive ("private information" would include date of birth, government issued identification material, bank account numbers, credit card numbers, financial transaction information, biometric information, medical information, security related details, etc).

Ministry of Citizens' Services

- *Collection* - Revise the collection provision to clearly state the point at which collection occurs.

Ministry of Health Services and Healthy Living and Sport

- *Adjust public body framework* - Amend the Act to recognize the changes to the "Health Sector" by defining "health care body" to reflect a "health sector family" model. Under this proposed model, the Ministry of Health Services would be the "parent" public body for the health sector with pre-eminent authority over the information necessary to manage the system; health authorities which play a subsidiary role in the management of the delivery of services in partnership with the ministry would form a "constellation" of bodies below the Ministry and these "child" bodies would take direction from the Ministry.