

The Freedom of Information and Protection of Privacy Act
and
Law Enforcement

Saskatchewan Access and Privacy Conference

April 18, 2007

Sandra Barreth

Portfolio Officer

Office of the Saskatchewan Information and Privacy Commissioner

TABLE OF CONTENTS

| | |
|---|----|
| Introduction | 1 |
| Purpose and Importance of the Legislation | 1 |
| Applicable Saskatchewan Legislation | 3 |
| The Freedom of Information and Protection of Privacy Act (FOIP) and The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP) | 3 |
| General Observations about Saskatchewan’s Access and Privacy Legislation | 5 |
| Structure of FOIP | 6 |
| Interpreting Access and Privacy Legislation | 6 |
| Exemptions | 8 |
| Exemption Criteria | 8 |
| FOIP Mandatory Exemptions | 9 |
| FOIP Discretionary Exemptions | 9 |
| Law Enforcement Exemption | 11 |
| Saskatchewan Provision | 14 |
| Disclosures and General Access and Privacy Limiting Rules | 18 |
| Conclusion | 21 |

Introduction

Privacy is a broad concept that is not defined in the legislation that regulates and influences our privacy rights or in the *Charter of Rights and Freedoms*¹ [hereinafter Charter]. “*Privacy is a fundamental human right. It's a critical element of a free society - as Justice La Forest of the Supreme Court once said, it's 'at the heart of liberty in a modern state.' ... There's no real freedom without privacy. In fact, some people call privacy 'the right from which all others flow.' A private sphere of thought and action, one that's your business and no one else's, it is fundamental to freedom of thought, freedom of conscience, freedom of speech, and so on.*”² It is important that we remember this and weigh it accordingly when balancing this fundamental, democratic right to privacy with our right to open, transparent, accountable government.

Purpose and Importance of the Legislation

Parliament has provided access and privacy legislation as a tool to ensure our right to open, transparent, and accountable government. The courts have noted that the *Access to Information Act*³ [hereinafter ATIA] “*is necessary because experience has shown that governments will not respect the right to information without a legal requirement to do so.*”⁴ With enactment of the ATIA and the *Privacy Act*,⁵ Parliament made a conscious decision to “*swing the pendulum away from an absolute confidentiality which the government enjoyed in areas such as federal-provincial relations and towards disclosure of all documents under Government control with only narrow and limited exceptions.*”⁶

¹ *Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11 [hereinafter Charter]

² Julien Delisle, Address (Ottawa Centre for Research and Innovation, GOL – OCRI Series, Ottawa, Ontario, June 4, 2003); available at http://www.privcom.gc.ca/speech/2003/02_05_a_030604_e.asp

³ *Access to Information Act*, R.S.C. 1985, c. A-1 [hereinafter ATIA]

⁴ *Canada (Information Commissioner) v. Canada (Prime Minister)* (1992), [1993] 1 F.C. 427 (Fed. T.D.) at 282

⁵ *Privacy Act*, R.S.C. 1985, c. P-21

⁶ *Canada (Information Commissioner) v. Canada (Prime Minister)* (1992), [1993] 1 F.C. 427 (Fed. T.D.) at 476-477

The Courts have determined that the rights embedded in access and privacy legislation are fundamental, democratic rights and have granted those Acts “quasi-constitutional” status. This means that the rights found in those Acts, while not clearly stated in the Charter, can be inferentially found in section 7 (right to life, liberty and security of the persons) and section 8 (right to be free from unreasonable search and seizure) of the Charter.⁷ The Supreme Court has quoted with approval the following statement:

*This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.*⁸

In fact, former Supreme Court Justice Gerard V. La Forest stated in the Report of the Special Advisor to the Minister of Justice, November 15, 2005, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*:

- *The Access to Information Act gives individuals a right of access to government information. The Privacy Act permits them to gain access to information about themselves held in government data banks, and limits government’s ability to collect, use and disclose such information...*
- *The rights protected by both Acts are of the highest importance in the functioning of a modern democratic state...So important is the right to government information that some have come to refer to it as ‘quasi-constitutional’ in nature... ”⁹*

⁷For a comprehensive discussion on this subject, see [Investigation Report No. H-- 2005 --002](http://www.oipc.sk.ca); available at www.oipc.sk.ca under Reports. There is also a good discussion of privacy and the Charter and, more particularly section 7, in the report of Mr. David Loukidelis, Information and Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act—Implications for British Columbia Public Sector Outsourcing*; available at <http://www.oipc.bc.ca/>.

⁸ *Dyment*, [1988] 2 S.C.R. 417 at 22

⁹ *Nautical Data International Inc. v. Canada (Minister of Fisheries and Oceans)*, 2005 FC 407 at para. 8; *Canada (Attorney General) v. Canada (Information Commissioner)*, [2004] 4 F.C.R. 181 at para. 20, 255 F.T.R. 56, 15 Admin. L.R. (4th) 58, 32, C.P.R. (4th) 464, 117 C.P.R. (2d) 85, 2004 FC 431, rev’d (2005), 253 D.R.R. (4th) 590, 335 N.R. 8, 40 C.P.R. (4th) 97, 2005 FCA 199, leave to appeal to S.C.C. requested; *Canada (Attorney General) v. Canada (Information Commissioner)*, [2002] 3 F.C. 630 at para. 20, 216 F.T.R. 247, 41 Admin. L.R. (3d) 237, 2002 FCT 128, 3430901 *Canada Inc. v. Canada (Minister of Industry)*, [2002] 1 F.C. 421 at para. 102, (2001), 282 N.R. 284, 45 Admin. L.R. (3d) 182, (2001) 14 C.P.R. (4th) 449, 2001 FCA 254, leave to appeal to S.C.C. refused, [2001] S.C.C.A. No. 537 (Q.L.)

- *The courts have also described the Privacy Act as carrying a ‘quasi-constitutional mission’.*¹⁰

This quasi-constitutional status means that access and privacy laws are special and enjoy a privileged status wherein they are typically paramount to other legislation. Our Saskatchewan legislation is closely modeled on the federal ATIA and *Privacy Act* and enjoys similar paramountcy provision. The importance of the rights protected by this legislation must always be kept in mind whenever we deal with the provisions of and interpret the requirements of this legislation.

Applicable Saskatchewan Legislation

Saskatchewan access and privacy legislation includes *The Privacy Act* (Saskatchewan), *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), and *The Health Information Protection Act* (HIPA).¹¹ The Office of the Saskatchewan Information and Privacy Commissioner (OIPC) oversees FOIP, LA FOIP and HIPA. In this analysis, we focus on the application of FOIP and LA FOIP; in particular, the law enforcement provisions in these Acts.

The Freedom of Information and Protection of Privacy Act (FOIP) and The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP)

FOIP applies to government institutions including government departments, boards, commissions, agencies and Crown corporations.¹² A list of the “*Boards, Commissions, Crown Corporations and*

¹⁰ *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, (2002) SCC 53 at para 25: “The Privacy Act is a reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society.” Also see: *R. v. Dymont*, [1988] 2 S.C.R. 417; *R. v. Mills*, [1999] 3 S.C.R. 668; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 402; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Edward*, [1996] 1 S.C.R. 128; *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66, 2003 SCC 8

¹¹ *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01 [hereinafter FOIP], Part IV; *The Local Authorities Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. L-27 [hereinafter LA FOIP], Part IV; *The Health Information Protection Act*, S.S. 1999, H-0.021; oversight provided by the Office of the Saskatchewan Information and Privacy Commissioner.

¹² FOIP, s. 2(1)(d)

Other Bodies” subject to FOIP can be found in the Appendix to the FOIP Regulation.¹³ There are more than 75 government institutions including every department of Executive Government, Crown corporations, and a number of provincial boards, commissions and agencies.

LA FOIP applies primarily to four types of organizations: (1) regional health authorities; (2) school divisions; (3) colleges and universities; and (4) municipalities of all types. These bodies are captured by the definition of “local authority”.¹⁴ In addition the LA FOIP Regulations enumerate another 27 organizations that also qualify as local authorities.¹⁵

Neither FOIP nor LA FOIP have a purpose or object clause. The Saskatchewan Information and Privacy Commissioner [hereinafter the Commissioner] has described the object of the statutes in the following terms:

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

- (a) giving the public a right of access to records;*
- (b) giving individuals a right of access to, and a right to request corrections of, personal information about themselves;*
- (c) specifying limited exceptions to the rights of access;*
- (d) preventing the unauthorized collection, use or disclosure of personal information by public bodies; and*
- (e) providing for an independent review of decisions made under this Act.¹⁶*

As noted earlier, FOIP and LA FOIP each have a paramountcy provision that provides that these two statutes are paramount in the event of a conflict with provisions in another provincial statute

¹³ *The Freedom of Information and Protection of Privacy Regulations*, c. F-22.01, Reg 1, Appendix, Part I

¹⁴ LA FOIP, s. 2(f)

¹⁵ *The Local Authority Freedom of Information and Protection of Privacy Regulations*, c. L-27.1, Reg 1, s. 3(1) and 3(2)

¹⁶ OIPC, *Review Report 2004-003*; *Review Report 2005 – 003*; available at www.oipc.sk.ca under Reports

unless the other statute is expressly declared to prevail over FOIP or LA FOIP.¹⁷ If another statute conflicts with and prevails over FOIP, the OIPC would not have jurisdiction to review or investigate the decisions or practices called into question.

Some records are excluded from the application of FOIP. Examples include published material, public records or material in the custody of The Saskatchewan Archives Board.¹⁸ FOIP does not apply to records of private industry or the Courts.

General Observations about Saskatchewan's Access and Privacy Legislation

To some extent, all three provincial access and privacy laws (FOIP, LA FOIP, HIPA) reflect the ten 'fair information practices or fair information principles.' These principles are described in the Canadian Standards Association *Model Code for the Protection of Personal Information* (hereinafter Model Code).¹⁹ The Model Code has been incorporated into Schedule 1 to the *Personal Information Protection and Electronic Documents Act*.²⁰

The FOIP and LA FOIP Acts address consent differently than the fair information principles. The Model Code is consent driven since it was primarily designed for the private sector. On the other hand, under both FOIP and LA FOIP Acts, consent is not required for the collection, use or disclosure of personal information for the mandated purposes of the government institutions or local authorities. Consent would only be required for collection, uses and disclosures that cannot clearly be tied to the mandated purpose of those public bodies.

¹⁷ FOIP, s. 23; LA FOIP, s. 22; For a more detailed analysis on how paramountcy provisions work, see the *OIPC Submission to the Workers' Compensation Board Review Committee*, available at www.oipc.sk.ca, under the What's New tab.

¹⁸ FOIP, s. 3

¹⁹ CSA, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96; also, see J.J. Edwards, *Human Resources Guide to Workplace Privacy*, (Canada Law Book, 2003), c. 2; and Information and Privacy Commissioner of Ontario, "Workplace Privacy: The Need for a Safety-Net," (November 1993); available at http://www.ipc.on.ca/scripts/index.asp?action=31&N_ID=1&P_ID=11439&U_ID=0 : "The code of fair information practices is an internationally recognized standard regarding the protection of informational privacy."

²⁰ PIPEDA, Schedule 1 (*Section 5*); Principles set out in The National Standard of Canada Entitled *Model Code for the Protection of Personal Information*.

This paper will focus primarily on the application of FOIP. Though similar to FOIP, there are some minor differences in LA FOIP and it will be necessary to consult LA FOIP to determine the material differences between the two statutes.

Structure of FOIP

FOIP has eight parts:

- Part I deals with interpretation, exclusions and the preservation of “existing rights”.
- Part II governs access to records.
- Part III defines both mandatory and discretionary exemptions to the right of access.
- Part IV deals with protection of the privacy of Saskatchewan residents and the confidentiality of their personal information.
- Part V outlines a procedure to deal with intervention by third parties in a decision to release records.
- Part VI creates the OIPC.
- Part VII defines the procedure for a formal review by the Commissioner and a further limited right of appeal to the Court of Queen’s Bench.
- Part VIII deals with general matters such as the burden of proof, exercise of powers by a surrogate, immunity from prosecution, offences and penalties.

Interpreting Access and Privacy Legislation

We sometimes get questions as to how we interpret the three laws that the OIPC oversees. Why does our interpretation sometimes differ from the dictionary or ordinary meaning of certain words? The answer is that the OIPC, consistent with other privacy and access oversight agencies in Canada, follows the “modern principle” in interpreting these laws. This has been described by the Alberta Information and Privacy Commissioner, quoting the Supreme Court of Canada,²¹ as follows:

²¹ AB IPC, *Order H2006-002*, at para 27: The “modern principle” has been consistently adopted by the Supreme Court of Canada as the preferred approach to the interpretation of legislation (see, for example, *Canada 3000 Inc.*,

The “modern principle” says I must read the words in an enactment “in their entire context and in their grammatical and ordinary sense harmoniously with the scheme of the Act, the object of the Act and the intention of Parliament”²²

In Saskatchewan, we are also guided by section 10 of *The Interpretation Act, 1995*²³ that provides:

10 Every enactment shall be interpreted as being remedial and shall be given the fair, large and liberal construction and interpretation that best ensure the attainment of its objects.

To give effect to this modern principle of statutory interpretation, we consider the way that the courts have been treating access to information and privacy legislation and the Charter as well as the purpose and unique nature of these laws. We are guided also by the approach taken by other Information and Privacy Commissioners since such laws across our nation have far more in common than they exhibit differences. It is useful to recognize that in the course of more than 20 years of Canadian experience with privacy and access law that certain terms have acquired particular meanings.²⁴

Re; Inter-Canadian (1991) Inc. (Trustee of), 2006 SCC 24 (CanLII) (SCC), June 9, 2006, para 36; H. J. Heinz Co. of Canada Ltd. v. Canada (Attorney General), [2006] 1 S.C.R. 441, 2006 SCC 13 (CanLII) (SCC), April 21, 2006; appeal from Alberta in ATCO Gas & Pipelines Ltd. v. Alberta (Energy & Utilities Board), 2006 SCC 4 (CanLII) (SCC), February 9, 2006, para 37.

²² Alberta IPC Order H2006-002, [28]. See also Ontario IPC Order PO-1879, British Columbia IPC Ruling File No. 15884, Alberta Adjudication Order #3 (Review Numbers 2170 and 2234)

²³ *The Interpretation Act, 1995*, c. I-11.2

²⁴ For example, the Supreme Court of Canada upheld the Ontario Commissioner’s interpretation of, and test for, advice and recommendations. [*Ontario (Ministry of Northern Development and Mines) v. Doe*, 2003 CanLII 3080 (ON S.C.D.C.); *Ontario (Ministry of Northern Development and Mines) v. Mitchinson*, 2005 CanLII 34229 (ON C.A.); *Ministry of Northern Development and Mines v. Tom Mitchinson, Assistant Commissioner and John Doe, Requirer*, 2006 CanLII 11833 (S.C.C.); and *Ontario (Ministry of Transportation) v. Cropley*, 2004 CanLII 11768 (ON S.C.D.C.); *Ontario (Ministry of Northern Development and Mines) v. Mitchinson*, 2005 CanLII 34229 (ON C.A.); *Ministry of Transportation v. Laurel Cropley, Adjudicator, Consulting Engineers of Ontario, Affected Party*, 2006 CanLII 11832 (S.C.C.)]

Exemptions

Access and privacy rights are not absolute. In terms of access to information, there are situations wherein it is appropriate for access to be denied to all or part of a record. These are prescribed exemptions to the right of access.

Exemption Criteria

The important nature of the legislation demands that any exemptions be clearly defined, necessary, limited and specific.²⁵ The ATIA clearly states “... *that necessary exemptions to the right of access should be limited and specific ...*”²⁶ The courts have fully supported these requirements.²⁷ To comply with the spirit of legislation premised on the right of access to records under the control of a government institution, it is essential that any necessary exemption be interpreted narrowly. In speaking to interpreting the ATIA, MacDonald J.A. aptly noted “... *all exemptions to access must be limited and specific. This means that where there are two interpretations open to the court, it must, given Parliament’s stated intention, choose the one that infringes on the public’s right to access the least. It is only in this way that the purpose of the Act can be achieved. It follows that an interpretation of an exemption that allows the government to withhold information from public scrutiny weakens the stated purpose of the Act.*”²⁸ These observations apply equally to our Saskatchewan access and privacy legislation.

²⁵ Treasury Board of Canada Secretariat, *Access to Information and Privacy Guidelines*; available at: www.tbs-sct.gc.ca (accessed May 11, 2006): Canadians require access to a wide range of information about government. There is a compelling public interest in openness, to ensure that the government is fully accountable for its goals and that its performance can be measured against these goals. This renders the government more accountable to the electorate and facilitates informed public participation in the formulation of public policy. It ensures fairness in government decision-making and permits the airing and reconciliation of divergent views across the country. The Guidelines provide a basis for balancing this principle of openness with the need to protect particular state and private interests expressed in the exclusion and exemption provisions of the legislation.

²⁶ ATIA, section 2(1)

²⁷ *Northern Cruiser Co. v. R.* (1992), 47 F.T.R. 192 (Fed T.D.), affirmed (1995) 185 N.R. 391 (Fed. C.A.)
Rubin v. Canada (Minister of Transport) (1997), 221 N.R. 145 (Fed. C.A.); *Canada Post Corp. v. Canada (Minister of Public Works)*, [1993] 3 F.C. 320 (Fed T.D.), affirmed [1995] 2 F.C. 110 (Fed. C.A.); *Noel v. Great Lakes Pilotage Authority Ltd.* (1987), [1988] 2 F.C. 77 (Fed. T.D.) at 80: ... the absolutely essential exceptions to this right must be specific and limited.; *St. Joseph Corp. v. Canada (Public Works & Government Services)*, [2002] F.C.J. No. 361, 2002 FCT 274, 2002 CarswellNat 573, 2002 CarswellNat 1296 (Fed. T.D.)

²⁸ *Rubin v. Canada (Minister of Transport)* (1997), 221 N.R. 145 (Fed. C.A.)

One area that may require limits on access to information includes national security and law enforcement investigations. I have dealt with these two areas of concern together as there are similar considerations that apply to each. National security has become highly visible in light of recent terrorist activity. However, many of the issues arising from national security concerns also apply to law enforcement investigations.

FOIP Mandatory Exemptions

There are four mandatory exemptions under FOIP. In these cases, the government institution has no alternative but to refuse access. These exemptions consist of the following:

- records from other governments;²⁹
- executive council confidence;³⁰
- third party information;³¹ and
- personal information of someone other than the applicant.³²

FOIP Discretionary Exemptions

In addition to the four mandatory exemptions, there are seven discretionary exemptions to disclosure:

- information injurious to intergovernmental relations or national defence;³³
- law enforcement and investigations;³⁴

²⁹ FOIP, s. 13; LA FOIP, s. 13

³⁰ FOIP, s. 16

³¹ FOIP, s. 19; LA FOIP, s. 18

³² FOIP, s. 29; LA FOIP, s. 28

³³ FOIP, s. 14; LA FOIP, s. 15 exempts documents of a local authority

- advice from officials;³⁵
- economic and other interests;³⁶
- testing procedures, tests and audits;³⁷
- danger to health or safety;³⁸ and
- solicitor-client privilege.³⁹

Before exercising a discretionary power the government institution must assess the following elements:

- the relevant facts and circumstances;
- the applicable law, including the objects of the law and the scope of the discretionary power; and
- how to properly apply the law to the relevant facts.

A government institution that uses a discretionary exception must first undertake two exercises:

- it must determine whether an exemption applies; and
- it must decide whether that information should nevertheless be disclosed, even though the exemption applies.

When exercising its discretion the government institution must consider the objects and purposes of FOIP. It must show that it considered all relevant factors. It must act in good faith, for a proper purpose and base the exercise of its discretion on relevant considerations only.

³⁴ FOIP, s. 15; LA FOIP, s. 14

³⁵ FOIP, s. 16; LA FOIP, s. 16

³⁶ FOIP, s. 18; LA FOIP, s. 17

³⁷ FOIP, s. 20; LA FOIP, s. 19

³⁸ FOIP, s. 21; LA FOIP, s. 20

³⁹ FOIP, s. 22; LA FOIP, s. 21

Law Enforcement Exemption

There is no doubt that information used in law enforcement and for national security can be particularly sensitive and prejudicial. Also, untimely disclosure of information may imperil the successful conclusion of an investigation or negotiation. At both the federal level⁴⁰ and the provincial level, the special concerns and needs in dealing with national security and law enforcement are dealt with as an exemption.

It is important to note early on that Saskatchewan residents face a rather unique circumstance with regard to law enforcement shared only by Prince Edward Island. In all other jurisdictions in Canada, local municipal police are subject to access and privacy legislation. In Saskatchewan, an interesting dichotomy exists wherein law enforcement may or may not be subject to access and privacy legislation depending upon where you live. If the RCMP provides policing services in your area, you have access to information about you in the possession or control of the RCMP in accordance with the federal access and privacy legislation. If you are subject to local, municipally provided policing services, you do not have the benefit of access and privacy legislation. In the result, in those Saskatchewan communities you do not have a right of access to information that the police may hold about you or the right to have errors corrected.

The Treasury Board of Canada Secretariat has provided substantial guidance on the application of the law enforcement exemption under the federal *Privacy Act*.⁴¹ As our legislation so closely

⁴⁰ John M. Reid, “*Response to the Report of the Access to Information Review Task Force, A Special Report to Parliament*” (Minister of Public Works and Government Services, Canada September, 2002) at 65: The Information Commissioner has stated, “There can be no justification for secrecy unless a reasonable expectation of injury to an important interest can be demonstrated. This axiom applies to enforcement and intelligence as to any other area. A decade of experience with the law has shown no compelling reason why such interests should get a 20-year grace period during which secrecy may be maintained without any need to demonstrate an injury from disclosure. ... The recommended changes will bring the federal Act into line with the law enforcement provisions in Ontario, British Columbia and Alberta.”

⁴¹ Treasury Board of Canada Secretariat, *Access to Information and Privacy Guidelines*; available at: www.tbs-sct.gc.ca (accessed May 11, 2006): *Law Enforcement*: This personal information is protected with a class test because of the difficulty in applying an injury test exemption to law enforcement records, since virtually all personal information in these records is of a sensitive nature and there is a large volume of requests in this area. Three conditions must be met before the exemption can be claimed:

parallels the requirements of the *Privacy Act*, this guidance is germane to our interpretation of FOIP.

The importance of the right of privacy was recognized in the *Criminal Code*.⁴² As Drapeau and Racicot observed,

...
*The Protection of Privacy Act, S.C. 1973-74, c. 50 was enacted as Part IV.1 of the Criminal Code, R.S.C. 1970, c. 34, imposing conditions to safeguard the public's interest in privacy within the sanctuary of a private dwelling and making it an offence to intercept private communications, disclose private communications and to possess equipment of the purpose of intercepting private communications except only as permitted by a superior court judge for purposes of law enforcement. **When an invasion of privacy becomes necessary in the course of a police investigation, the police must seek an authorization and give the judge highly specific information so that he can properly exercise his discretion to set limits on unnecessary intrusions on privacy.***⁴³
[emphasis added]

The Ontario Commissioner reviewed the legislative history of the law enforcement exemption in Ontario Privacy Complaint Report MC-040012-1 and held as follows:

-
- (a) The exemption can be claimed only where the personal information has been obtained or prepared by the limited number of investigative bodies listed in the regulations.
 - (b) The exemption can be applied only to personal information obtained or prepared by such an investigative body in the course of a lawful investigation. This means that the investigation must be authorized by or pursuant to a particular law. It is not sufficient to say that any investigation which is not unlawful is considered to be lawful. This does not, however, address the issue of the legality of techniques used during a lawful investigation. Nor does this address the issue of whether or not evidence has been legally obtained.
 - (c) The exemption applies only to personal information obtained or prepared by such an investigative body in the course of lawful investigations pertaining to:
 - the detection, prevention or suppression of crime;
 - the enforcement of any law of Canada or a province; or
 - activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*.

This last provision limits the application of the exemption to personal information obtained during the conduct of investigations relating to crime or law enforcement.

Injury to the conduct of lawful investigations: This exemption protects the integrity and effectiveness of investigations which are not law enforcement investigations. An example might be investigations conducted to determine the cause of an accident, but not to lay charges or assess blame.

⁴² R.S., 1985, c. C-46

⁴³ Drapeau, Colonel Michel W. and Racicot, Marc-Aurele, *Federal Access to Information and Privacy Legislation Annotated 2006*, 3. *Protection of Privacy Act – Criminal Code*, (Toronto: Thomson Canada Limited, 2005) at 6-5

*The legislative history of section 32(f)(ii) supports this interpretation. In discussing the need to allow law enforcement agencies from different jurisdictions to share personal information, the report entitled **Public Government for Private People: The Report of the Commission on Freedom of Information and Individual Privacy 1980, vol.3** (Toronto: Queen's Printer, 1980) (the Williams Commission Report) stated (at p.701):*

*...The account of law enforcement information systems in Ontario published in a Commission research paper indicates the existence of information-sharing practices among federal, provincial, municipal, and even foreign law enforcement agencies. Clearly, such cooperative efforts are instrumental in the apprehension of criminals, and it would be unwise, in our view, to preclude information exchanges for that purpose. Such information will not normally be submitted voluntarily by the data subject in the first place. **Information gathered in the course of an investigative activity will most commonly be shared in order to secure assistance from other law enforcement officials who may have an opportunity to apprehend suspected parties. Accordingly, we recommend that such exchanges be exempt from the no-transfer rule.***

It appears from the language used by the Williams Commission that the purpose of allowing transfers of personal information between law enforcement agencies is to further law enforcement purposes, rather than to allow unfettered, discretionary exchanges of information for any purpose.

In addition, related provisions in Part II of the Act that permit law enforcement agencies to handle personal information contain law enforcement purpose limitations. For example, section 28(2) reads, in part:

No person shall collect personal information on behalf of an institution unless the collection is...used for the purposes of law enforcement...

Section 29(1)(g) reads:

An institution shall collect personal information only directly from the individual to whom the personal information relates unless, the information is collected for the purpose of law enforcement

*In my view, it would be inconsistent and irrational for the legislature to have intended that law enforcement agencies may rely on section 28(2) and 29(1)(g) only where the collection is for law enforcement purposes, **yet permit those same agencies to share information with each other for any purpose whatsoever, even if unrelated to a law enforcement purpose.***

...

This interpretation also is consistent with one of the fundamental purposes of the Act, which is "to protect the privacy of individuals with respect to personal information about themselves held by institutions" [section 10] [emphasis added]

When considering application of the law enforcement exemption, the public body must take this historical perspective into account.

Saskatchewan Provision

FOIP provides a law enforcement exemption to the right of access to government records in Part III. Section 15 provides the authority for this exemption as follows:

Law enforcement and investigations

15(1) A head may refuse to give access to a record, the release of which could:

- (a) prejudice, interfere with or adversely affect the detection, investigation, prevention or prosecution of an offence or the security of a centre of lawful detention;*
- (a.1) prejudice, interfere with or adversely affect the detection, investigation or prevention of an act or omission that might constitute a terrorist activity as defined in the Criminal Code;*
- (b) be injurious to the enforcement of:*
 - (i) an Act or a regulation; or*
 - (ii) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada;*
- (c) interfere with a lawful investigation or disclose information with respect to a lawful investigation;*
- (d) be injurious to the Government of Saskatchewan or a government institution in the conduct of existing or anticipated legal proceedings;*
- (e) reveal investigative techniques or procedures currently in use or likely to be used;*
- (f) disclose the identity of a confidential source of information or disclose information furnished by that source with respect to a lawful investigation or a law enforcement matter;*
- (g) deprive a person of a fair trial or impartial adjudication;*
- (h) facilitate the escape from custody of an individual who is under lawful detention;*
- (i) reveal law enforcement intelligence information;*
- (j) facilitate the commission of an offence or tend to impede the detection of an offence;*
- (k) interfere with a law enforcement matter or disclose information respecting a law enforcement matter;*
- (l) reveal technical information relating to weapons or potential weapons; or*
- (m) reveal the security arrangements of particular vehicles, buildings or other structures or systems, including computer or communication systems, or methods employed to protect those vehicles, buildings, structures or systems.*

- (2) Subsection (1) does not apply to a record that:
- (a) provides a general outline of the structure or programs of a law enforcement agency; or
 - (b) reports, by means of statistical analysis or otherwise, on the degree of success achieved in a law enforcement program.

The OIPC has addressed the interpretation of the law enforcement exemption, specifically clause 15(1)(c), in Reports F-2006-004, F-2006-001, and F-2004-006.⁴⁴

In Report F-2006-001, the Commissioner considered the quasi-constitutional nature of FOIP and the direction of the Saskatchewan Court of Appeal in *General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance*⁴⁵ that the basic policy of the Act is that “disclosure, not secrecy is the dominant objective of the Act”. The Commissioner then defined “lawful investigation” to mean an investigation that is authorized or required and permitted by law.⁴⁶ The Commissioner also reviewed some of the characteristics of proceedings under other statutes that qualify as a lawful investigation.

A government institution cannot invoke section 15(1)(c) of FOIP unless there is an active and ongoing investigation.⁴⁷ The Commissioner advised that “[w]e view both parts of section

⁴⁴ Available at www.oipc.sk.ca under Reports

⁴⁵ [1993] S.J. No. 601 at [11]

⁴⁶ OIPC, Report F-2006-001; available at www.oipc.sk.ca under Reports:

[24] In Saskatchewan OIPC Report 2004-006, this office defined “lawful investigation.”

“[26] The term “lawful investigation” is not defined in the Act. It was considered by Saskatchewan’s first Information and Privacy Commissioner, Mr. Derril McLeod, in his Report 93-021. In that case, he chose to define “lawful investigation” to mean an investigation that is authorized or required and permitted by law. He received a submission from the government institution that “lawful investigation” should mean any investigation that is not contrary to or prohibited by law. Commissioner McLeod stated, in response, However, if this were so, it would encompass any and every investigation of any matter whatsoever not prohibited by some specific law. I am unable to conclude that such a broad interpretation is intended or warranted. In my view, the expression “lawful investigation” means an investigation that is authorized or required and permitted by law. So also, the expression, “law enforcement” must, in my view, be considered to pertain to enforcement of laws of general or particular application by appropriate law enforcement agencies, and not to the determination of private issues or rights between parties to a contract as appears to be the case here. [page 6]”

[27] We adopt the same definition of “lawful investigation”.

⁴⁷ Gary Dickson, *Access to Information - Statutory Alternatives* (Canadian Bar Association (Saskatchewan) Mid-Winter Meeting, February 2, 2007); available at www.oipc.sk.ca under What’s New; also see Report F-2004-006, Report F-2006-001 and Report 2006-004; available under Reports

15(1)(c) of the Act to denote the same meaning of lawful investigations. If the legislature had intended a different meaning, then different words would have been used. The two parts of the subsection will only apply if there is an active investigation underway.”⁴⁸ Therefore, the same tests apply equally to both parts of the exemption whether the claim of exemption relates to interference with or disclosure of information with respect to a lawful investigation. In Report F-2004-006, the Commissioner determined that “it is possible to disclose information with respect to a lawful investigation without interfering with a lawful investigation.” The Commissioner has held that the test for claims of the section 15(1)(c) exemption for law enforcement investigations should be limited to open investigations.⁴⁹ The Newfoundland Commissioner accepted and adopted this approach in his *Report 2007-003, Memorial University of Newfoundland*.⁵⁰

In Report F-2006-001, the Commissioner also addressed the issue of whether FOIP captures records produced by another investigative body, but in the possession of a public body covered by FOIP. The Commissioner found as follows:

[26] ... In our Report 2004-006 we canvassed this issue in paragraphs [56] to [61]. We concluded that

“... a record may be “information with respect to a lawful investigation” in circumstances where the record in full or in part has been created by another body. I find no requirement in the Act that this exemption can only be invoked in circumstances where the investigation has been solely the work of the government institution. The key is whether the record is in the possession or under the control of the government institution.”

[27] As a consequence, all material received by the OFC to the extent that it is in the possession or under the control of CPS is subject to the access request in this case. In this case, the records in question are in the possession of the OFC and therefore in the possession of CPS. It follows that records of another body’s investigation are not exempt because they are in the possession of CPS.

⁴⁸ SK OIPC, *Report F-2006-004*, at [27], quoting *Report F-2006-001* at [41]; available at www.oipc.sk.ca under Reports

⁴⁹ SK OIPC, *Report F-2006-001*; available at www.oipc.sk.ca under Reports

⁵⁰ Newfoundland IPC, *Report 2007-003*; available at http://www.oipc.gov.nl.ca/pdf/Report%202007-003_MUN.pdf

[28] *The above would also apply in this circumstance to all material received by the OFC even if prepared by another entity.*

All records in the possession or control of the public body are subject to FOIP⁵¹ whether or not they are created by the public body. Note that records in the possession of a contractor to the public body remain subject to FOIP by virtue of their connection to the public body and the public body's retained control over those records.⁵²

When claiming the law enforcement exemption under FOIP, or any other exemption to deny access to a record, FOIP clearly places the burden to establish that exemption on the public body.⁵³ Meeting the burden of proof requires more than a general assertion that the exemption applies. Justice Gonthier said the following about the Official Languages Commissioner's generalized fear of disclosure of investigative records:

“The appellant (Commissioner of Official Languages) does not rely on any specific fact to establish the likelihood of injury. The fact that there is no detailed evidence makes the analysis almost theoretical. Rather than showing the harmful consequences of disclosing the notes of the interview with Ms. Dube on future investigations, Mr. Langelier (for the Commissioner) tried to prove, generally, that if investigations were not confidential this could compromise their conduct, without establishing specific circumstances from which it could reasonably be concluded that disclosure could be expected to be injurious. ... In the case before us, the appellant has not succeeded in showing that it is reasonable to maintain confidentiality.”⁵⁴

Exemptions claimed must be supportable and supported. To meet the burden of proof, the Commissioner considers arguments that address the specifics of the circumstances and detailed evidence produced by the public body. Prior decisions of the Commissioner, decisions of other Information and Privacy Commissioners and legal case law are also persuasive and should be included when making your case for relying on an exemption. To rely on an exemption, each

⁵¹ FOIP, s. 5

⁵² For more information, see the SK OIPC, *A Contractor's Guide to Access and Privacy in Saskatchewan*; available at www.oipc.sk.ca under Resources

⁵³ FOIP, s. 61

⁵⁴ *Lavigne v. Canada (Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, (2002) SCC 53 at para 61

data element of the exemption must be met. The tests to meet the burden of proof have been dealt with extensively in numerous Commissioner Reports, available at www.oipc.sk.ca under Reports.

Disclosures and General Access and Privacy Limiting Rules

To date the OIPC has not had occasion to determine formally how the other sections of FOIP relating to law enforcement will be interpreted. However, in keeping with the Supreme Court of Canada's guidance, the OIPC will interpret exemptions in a narrow, specific and limited manner and in accordance with general access and privacy 'best practices.' This interpretive approach applies equally to disclosures under Part IV of FOIP.

Best practices consist of a set of limiting rules which set the stage for interpreting exemptions. Under access and privacy legislation, public bodies must collect the least amount of personal information necessary for an identified purpose. Where possible, the information should be collected directly from the individual to whom it relates. The public body should share personal information with only those who 'need to know' whether sharing internally or externally. FOIP formalizes these general rules in the following sections:

- section 25 (Purpose of information),
- section 26 (Manner of Collection),
- section 28 (Use of personal information), and
- section 29 (Disclosure of Personal Information).

FOIP also imposes a duty on a public body to ensure that information collected is "accurate and complete" (section 27). These sections have been reproduced in the legislation handout provided.

When collecting personal information, consider that the *Justice Information Privacy Guidelines*⁵⁵ states:

*“there should be some limits placed on the collection of personal information. Personal information should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. **It is important to remember that an individual’s knowledge and consent rights will be limited depending on his or her relationship to the justice system (e.g., suspect, offender, victim, witness, juror, or offender’s family). A test of relevance should also be applied (e.g., by an independent third party or as authorized in legislation) when collecting personal information on individuals without their knowledge or consent, or when the individual is not charged with a crime; i.e., under investigation, or when an investigative body is “information gathering”.***

[emphasis added]

The public body should collect personal information indirectly in very limited circumstances and only where it is not reasonably practicable to collect directly from the individual involved.⁵⁶

When considering an access request to which the law enforcement exemption may apply or a disclosure in accordance with clause 29(2)(g), consider whether all the elements of the section apply. For example, is the record is part of a “lawful investigation”?⁵⁷ Next, apply section 8 of FOIP in determining whether any portion of the record can be severed so as to release as much of the record as possible. Finally, consider whether or not to exercise the discretion available under FOIP.

⁵⁵ *Justice Information Privacy Guidelines*, (National Criminal Justice Association: September 2002) at 27: The guidelines were produced after a series of workshops involving privacy experts from Canada (including the Ontario IPC), the United Kingdom, and Australia.

⁵⁶ FOIP, s. 26(1)

⁵⁷ Government of Alberta, *Freedom of Information and Protection of Privacy Guidelines and Practices*, (2005, Government of Alberta Access and Privacy Branch, Edmonton): “An investigation relating to a breach of contract or a contravention of a policy by an employee will not normally constitute a law enforcement activity, since these actions would not result in a penalty or sanction under a statute or regulation.”

Also, consider Ontario IPC *Investigation Report MC-980044-1*: There is no question that “policing” is at the core of the law enforcement mandate of all Police Services. However, it does not necessarily follow that all actions taken by the Police constitute policing activities.

When applying the need to know principle, whether internal or external, consider the specific context of the request for information. In relation to law enforcement sharing practices, note that the Supreme Court of Canada, in *R. v. Dymont*,⁵⁸ stated:

*“The state’s interest in detecting and preventing crime begins to prevail over the individual’s interest in being left alone at the point where **credibly-based probability replaces suspicion**. History has confirmed the appropriateness of the threshold for subordinating the expectation of privacy to the needs of law enforcement. ... Quite simply, the constitution does not tolerate a **“low standard which validate intrusion on the basis of suspicion, and authorize fishing expeditions of considerable latitude”** (*Hunter v. Southam Inc.*, *supra*, at p. 167).”*
[emphasis added]

The Supreme Court of Canada provided further guidance in *R. v. Plant*⁵⁹ as follows:

Consideration of such factors as the nature of the information itself, the nature of the relationship between the parties releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained, and the seriousness of the crime being investigated allow for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement. It is, then, necessary to apply this contextual approach to the facts of the case at bar.”
[emphasis added]

When you contemplate disclosing to a law enforcement agency, consider whether authority exists for disclosure and whether an evidentiary basis has been established to justify the disclosure. Note that such a disclosure would be a “secondary use” of the information collected. Privacy best practices normally require that the public body obtain the consent of the individual whose personal information is being disclosed for a secondary purpose. Subsection 29(1) of FOIP requires the individual’s consent for disclosures of their personal information except in accordance with subsection 29(2) or section 30 discretionary disclosure provisions. Clause 29(2)(g) provides discretion to disclose to a “law enforcement agency” or “investigative body.” Note that if the public body is applying the section 29(2)(g) disclosure provision, the “law

⁵⁸ [1988] 2 S.C.R. 417

⁵⁹ [1993] 3 S.C.R. 281 at 8

enforcement agencies or investigative bodies” to which personal information may be disclosed are listed in section 14 of the FOIP Regulations.

Conclusion

FOIP provides the legislative framework for access to information in the government institution’s possession or control. It also defines the rules of the collection, use and disclosure of personal information. The right of access is limited by the law enforcement exemption and the other mandatory and discretionary exemptions in Part III. The right of privacy is limited by the list of discretionary disclosures in s. 29(2) of FOIP. In accordance with the direction from the Supreme Court of Canada and the Saskatchewan Court of Appeal, these exemptions are to be interpreted narrowly. The law enforcement exemption in Part III addresses protection of information which could impair lawful investigations. The collection, use and disclosure provisions in Part IV address situations wherein it is appropriate and necessary to share information with law enforcement. Proper application of the statutes ensures the balance between law enforcement requirements and the preservation of a free and just society such as we enjoy in Canada is considered.

APPENDIX ‘A’

Quasi-Constitutional Status

- From the Report of the Special Advisor to the Minister of Justice, Former Supreme Court Justice Gerard V. La Forest, November 15, 2005, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*:
 - “The Access to Information Act gives individuals a right of access to government information. The Privacy Act permits them to gain access to information about themselves held in government data banks, and limits government’s ability to collect, use and disclose such information ...”
 - “The rights protected by both Acts are of the highest importance in the functioning of a modern democratic state ... So important is the right to government information that some have come to refer to it as “quasi-constitutional” in nature ...”

[Nautical Data International Inc. v. Canada (Minister of Fisheries and Oceans), 2005 FC 407 at para.8; *Canada (Attorney General) v. Canada (Information Commissioner)*, [2004] 4 F.C.R. 181 at para. 20, 255 F.T.R. 56, 15 Admin. L.R. (4th) 58, 32, C.P.R. (4th) 464, 117 C.P.R. (2d) 85, 2004 FC 431, rev’d (2005), 253 D.R.R. (4th) 590, 335 N.R. 8, 40 C.P.R. (4th) 97, 2005 FCA 199, leave to appeal to S.C.C. requested; *Canada (Attorney General) v. Canada (Information Commissioner)*, [2002] 3 F.C. 630 at para. 20, 216 F.T.R. 247, 41 Admin. L.R. (3d) 237, 2002 FCT 128, 2430901; *Canada Inc. v. Canada (Minister of Industry)*, [2002] 1 F.C. 421 at para. 102, (2001), 282 N.R. 284, 45 Admin L.R. (3d) 182, (2001) 14 C.P.R. (4th) 449, 2001 FCA 254, leave to appeal to S.C.C. refused, [2001] S.C.C.A. No 537 (Q.L.)]

- The courts have also described the Privacy Act as carrying a “quasi-constitutional mission.”

[Lavigne v. Canada (Office of the Commissioner of Official Languages), [2002] 2 S.C.R. 773, (2002) SCC 53 at para 25; *R. v. Dymont*, [1988] 2 S.C.R. 417; *R. v. Mills*, [1999] 3 S.C.R. 668; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 402; *R. v. Plant*, [1993] 3 S.C.R. 281; *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Edward*, [1996] 1 S.C.R. 128; *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66, 2003 SCC 8]