foip bulletin

Number 7 | Revised March 2009

Law Enforcement

CONTENTS

Introduction	**1**
Definition of law enforcement	2
Information to which the Act does not apply	**3**
Access requests under Part 1	**4**
Harm to law enforcement	4
Unreasonable invasion of personal privacy	11
Harm to individual or public safety	12
Local public body confidences	12
Harm to intergovernmental relations	13
Refusal to confirm/deny existence of a record	13
Disclosure in the public interest	**14**
Privacy protection under Part 2	**15**
Disclosure not an unreasonable invasion of personal privacy	16
Disclosure authorized or required by law	16
Disclosure to assist in an investigation	16
Disclosure by a law enforcement agency	17
Collection of information from the private sector	**17**
Practical tips on managing law enforcement information	**18**

INTRODUCTION

The *Freedom of Information and Protection of Privacy Act* (the FOIP Act) is intended to promote accountability on the part of public bodies by providing a right of access to information and by controlling the manner in which public bodies collect, use and disclose personal information. Perhaps nowhere is the balance between competing public and private interests more important than in the area of law enforcement and public security.

The FOIP Act is not intended to impede authorized law enforcement activities or to prevent the sharing of personal information for the purposes of law enforcement investigations and proceedings. The Act is intended to ensure that law enforcement agencies and other public bodies operate under a consistent set of rules. These rules appear in a number of different contexts throughout the Act. This Bulletin is intended to supplement *FOIP Guidelines and Practices*, produced by Access and Privacy, Service Alberta, by providing an overview of the way the Act applies to law enforcement.

Topics addressed in this Bulletin are:

- the definition of "law enforcement" and the Commissioner's interpretation of the definition,
- the mandatory and discretionary exceptions to disclosure of personal information or other information in a law enforcement record in response to an access request under **Part 1**,
- the collection, use and disclosure of law enforcement information under **Part 2**,
- practical tips on the creation and management of law enforcement records.

Publications produced by Access and Privacy, Service Alberta, cited in this Bulletin are available on the FOIP website at foip.alberta.ca. Decisions, practice notes and publications issued by the Office of the

Information and Privacy Commissioner of Alberta may be found on the OIPC website at www.oipc.ab.ca.

Definition of "law enforcement"

The definition of "**law enforcement**" is critical to applying the Act.

1(h) "law enforcement" means

(i) policing, including criminal intelligence operations,

(ii) a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or

(iii) proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred.

(The present wording of **section 1(h)** is a result of amendments to the Act in May 1999. This should be kept in mind when referring to Orders of the Information and Privacy Commissioner in response to requests for review and complaints initiated before May 1999.)

"**Policing**" means activities, carried out under the authority of a statute, regarding the maintenance of public order, detection and prevention of crime, or the enforcement of law (*IPC Order 2000-027*).

For example, when an individual expresses to a police officer a fear for safety or a threat to either himself or another person, the matter is a "policing" matter and falls within the definition of "law enforcement" (*IPC Order F2006-002*).

"**Investigation**" has been defined, in general, as a systematic process of examination, inquiry and observation (*IPC Orders 96-019* and *F2002-024*).

A "**law enforcement investigation**" is expressly limited in **section 1(h)(ii)** to an investigation "that leads or could lead to a penalty or sanction." The Commissioner has ruled that, for the purposes of this definition, the public body must be authorized to conduct the investigation and the investigation must be one that can result in a penalty or sanction imposed under a statute or a regulation (*IPC Order 2000-023,* affirming *IPC Order 96-006*).

For the purposes of this interpretation, "**regulation**" is understood to mean a regulation as defined in section 1(1)(c) of the *Interpretation Act*. This includes a bylaw enacted under a statute (*IPC Investigation Report F2002-IR-009*).

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. (See *IPC Orders 2000-019, 2000-023* and *F2003-005*.)

The recruitment process for prospective police officers has been found to not be a law enforcement investigation. The possible dismissal or the withdrawal of an employment offer was not a legislated sanction or penalty (*IPC Order F2004-022*).

An investigation into a workplace accident conducted under the *Occupational Health and Safety Act* is a law enforcement investigation. An investigation can lead to penalties or sanctions under that Act (*IPC Order F2005-026*).

A law enforcement investigation may be a *police, security* or *administrative* investigation. These categories are not mutually exclusive and a law enforcement investigation may have different aspects provided that it meets the Act's definition of "law enforcement."

The investigating body does not have to impose the penalty or sanction, but can refer the matter to another body to impose the penalty or sanction.

The Commissioner has not commented on what constitutes a "**security investigation**." However, since the Commissioner has ruled that **section 1(h)(ii)** requires that the investigation lead or could lead to a penalty or sanction imposed under a statute or

regulation, an investigative activity relating to security that is conducted in accordance with a public body's policies, and not under a regulation, bylaw or resolution, would not fall within the definition of a law enforcement investigation.

A post-secondary institution's investigation of a possible contravention of its Code of Student Conduct relating to computer use may be considered a *security* investigation under the Act if the alleged conduct threatened the institution's computer system (as opposed to offending moral standards). Such an investigation is more likely to be considered a security investigation for the purposes of the Act if the investigation is conducted by a special constable in campus security services, perhaps with the assistance of a network security administrator, and not simply by a network administrator.

An "**administrative investigation**" refers to activities undertaken to enforce compliance or to remedy non-compliance with standards, duties and responsibilities imposed by statute or regulation. (See *IPC Orders 96-006* and *F2002-024*.)

Examples of administrative investigations include the following.

- An inspection under the *Water Act* since the Act provides for investigation and inspection powers and also includes penalties for non-compliance (*IPC Order F2002-024*).
- An investigation by Environment Canada into the discharge from a landfill site owned by a municipality (*IPC Order F2005-013*).
- Inquiries conducted by the Law Society of Alberta and the Chief Judge of the Provincial Court into complaints made to them about members. Sanctions could be imposed under sections 72 and 73 of the *Legal Profession Act* and section 34(2) of the *Judicature Act* (*IPC Order F2007-007*).
- An investigation under the *Traffic Safety Act* and the Operator Licensing and Vehicle Control Regulation to determine whether an individual could safely operate a motor vehicle. Possible sanctions included disqualification from driving and suspension or cancellation of vehicle registration (*IPC Investigation Report F2007-IR-004*).
- A complaint made and an investigation conducted under the *Protection of Persons in Care Act* (*IPC Order F2005-009*).

A "**complaint**" that triggers an investigation is part of the law enforcement investigation and therefore part of a law enforcement record. The intent of this provision is to ensure that the identity of a complainant can be protected in appropriate cases.

A "**proceeding**" is an action or submission to any court, judge or other body having authority, by law or by consent, to make decisions.

"**Law enforcement proceedings**" are proceedings that lead or could lead to a penalty or sanction under a statute or regulation. These include not only formal court proceedings but also proceedings of adjudicative or administrative tribunals, such as the Labour Relations Board. The penalty or sanction can be imposed by the public body conducting the proceeding or by another body to which the results of the proceedings can be referred.

In summary, the key to identifying a "law enforcement" activity is that

- the activity must be based on authority granted by statute or regulation, and
- the penalties or sanctions that can be imposed must be set out in a statute or regulation.

INFORMATION TO WHICH THE ACT DOES NOT APPLY

The FOIP Act does not limit the information available by law to a party to legal proceedings (**section 3(c)**). The process of disclosure in criminal proceedings, for example, is not limited by the Act. The Act also does not affect the power of a court or tribunal to compel a witness to testify or compel the production of documents (**section 3(d)**).

The FOIP Act does not apply to court records (**section 4(1)(a)**) or to records relating to a prosecution if all proceedings have not been completed (**section 4(1)(k)**). Other information relating to a law enforcement investigation or proceeding may also

be excluded under **section 4(1)**. See *FOIP Guidelines and Practices* for a discussion of these exclusions and their effect.

A number of other Alberta statutes and regulations contain provisions that further limit the application of the FOIP Act under the Act's provision for the paramountcy of other legislation (**section 5**). For example, section 16 of the *Mandatory Testing and Disclosure Act* prohibits disclosure of information obtained under that Act, despite the FOIP Act. See FOIP Bulletin No. 11: *Paramountcy*, produced by Access and Privacy, Service Alberta, for further information on processing requests for records in cases where paramountcy may be involved.

ACCESS REQUESTS UNDER PART 1

A public body that receives a request for records containing law enforcement information should always consider the source of the information and whether there may be a need to consult with other bodies.

It may be appropriate to transfer the request to another public body under **section 15** of the Act if:

- the record was produced by or for another public body,
- the other public body was the first to obtain the record, or
- the record is in the custody or under the control of the other public body.

A public body cannot transfer a request to a law enforcement agency that is not a public body as defined in the FOIP Act. For example, a public body cannot transfer a request to the RCMP, even when the RCMP is acting as a municipal police force, because the RCMP is subject to federal legislation. However, a public body may refer an applicant to the process for making a request to the RCMP under the federal *Access to Information Act* or the federal *Privacy Act.* A public body must nevertheless respond to the applicant's request unless the request is withdrawn.

In responding to a request, there are a number of exceptions to disclosure that may apply. The most significant are the exceptions for disclosure harmful to law enforcement (**section 20**), disclosure that may be an unreasonable invasion of personal privacy (**section 17**) and disclosure harmful to individual or public safety (**section 18**). If any of these exceptions apply, there may be grounds for refusing to confirm or deny the existence of information to which the exception applies (**section 12**).

Exceptions to disclosure are discussed in this section. This discussion includes consideration of the criteria that need to be met in order to apply the various exceptions and the evidence that would be required if there were a request for review by the Commissioner.

Harm to law enforcement

Section 20(1) is a discretionary ("may") exception. The exercise of discretion requires the public body to consider all relevant circumstances before deciding whether to withhold information that meets the criteria for an exception to disclosure.

Section 20(1) permits a public body to refuse to disclose information to an applicant if the disclosure could reasonably be expected to be harmful to law enforcement. This provision refers to "information," which may include personal information.

Records relating to law enforcement matters will typically be in the custody or under the control of law enforcement agencies. However, a public body that is the subject of a law enforcement investigation may also have records in its custody or under its control to which **section 20(1)** may apply. (*See IPC Order 2005-013.*)

Harm a law enforcement matter

Section 20(1)(a) allows a public body to refuse access to information that could reasonably be expected to harm a law enforcement matter.

This exception requires a public body to be able to demonstrate two things:

- that it is dealing with a "law enforcement matter" within the definition requirements of "law enforcement" discussed above, and
- that the disclosure would result in "harm" to that matter.

The test for "harm," as set out in *IPC Order 96-003*, has three elements.

- **Direct and specific harm**

  There must be a clear cause-and-effect relationship between the disclosure of the information and the harm alleged. The harm must be directly linked to the disclosure of the information and involve harm to a specific law enforcement matter. A public body may not take the approach that the release of any information from any investigative file is harmful to investigations generally.

- **A significant level of harm**

  The level of harm that is likely to result must constitute "damage" or "detriment" to the matter as opposed to simply causing a hindrance or minimal interference.

- **Reasonable probability of the harm occurring**

  The likelihood of the harm must be genuine and conceivable. A public body may not take an overly cautious approach or have a general concern that harm may occur because of the sensitivity of the information.

Many of the provisions in **section 20(1)** require the application of the harms test. See the discussion of the relevant provision in this Bulletin for examples of the application of the harms test. See also FOIP Practice Note 1: *Applying 'Harms' Tests* issued by the Office of the Information and Privacy Commissioner of Alberta.

Matters concerning the defence of Canada or its allies

Section 20(1)(b) was amended and **section 20(1)(b.1)** added in 2002 by the *Security Management Statutes Amendment Act.*

As amended, **section 20(1)(b)** allows a public body to refuse to disclose information that may prejudice the defence of Canada or any other foreign state allied to or associated with Canada. If a public body believes that it holds information to which this exception may apply, some consultation with other government agencies, such as the Department of National Defence, the RCMP or the Canadian Security Intelligence Service may be required.

Threats to the security of Canada

Section 20(1)(b.1) allows a public body to withhold information that could disclose activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act* (Canada) (the CSIS Act).

Section 2 of the CSIS Act defines what constitutes "threats to the security of Canada":

- espionage or sabotage, or supporting activities, against Canada or detrimental to the interests of Canada,
- foreign-influenced activities detrimental to the interests of Canada that are clandestine or deceptive or involve a threat to any person,
- activities within or relating to Canada that threaten or use acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective, and
- activities directed toward undermining or overthrowing the constitutionally established system of government in Canada by covert unlawful acts or violence.

These activities do not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the listed activities.

A public body relying on this exception to disclosure would need to be able to explain why disclosure of the information would be a threat to the security of Canada, as defined above. Consultation with other government departments or agencies that specifically deal with threats of this nature would be important if the public body's decision to withhold information were challenged.

Investigative techniques

Section 20(1)(c) allows a public body to refuse to disclose information if the disclosure could reasonably be expected to harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement.

In *Order F2007-005,* the Adjudicator defined the following terms.

- "**Investigative**" means "seeking or serving to investigate."
- "**Investigate**" means "inquire into, examine, study carefully; make a systematic inquiry or search; to make (a suspect) the subject of a criminal inquiry."
- "**Investigative techniques and procedures**" means "techniques and procedures used to conduct an investigation or inquiry for the purpose of law enforcement."

The Adjudicator stated that, while the pursuit and apprehension of a suspect may be consequences of an investigation, they do not form part of an investigation or inquiry process. Therefore a training video relating to the canine unit's method of searching for and apprehending suspects did not contain information about an investigative technique or procedure.

When applying **section 20(1)(c)**, the level of harm must be directly linked to the continued effectiveness of an investigative technique or procedure. If an investigative technique or procedure is commonly known to the public, revealing this technique or procedure will not be considered sufficient "harm" to allow a public body to rely on this exception. (See *IPC Orders 96-010, 99-010* and *F2003-005*).

For example, video surveillance is an investigative technique commonly known by the public to be used by law enforcement. Information concerning the fact that video surveillance is used would likely not be covered by this exception. **Section 20(1)(c)** has been applied to remove information concerning an investigative technique or procedure used in the conduct of a threat assessment done by a police service (see *IPC Order 2000-027*).

Confidential source

Section 20(1)(d) allows a public body to refuse to disclose information that may reveal the identity of a confidential source of law enforcement information.

The exception requires the public body to meet a three-part test:

- that "law enforcement" information is involved; the actual information that may reveal the identity of the confidential source does not necessarily have to be law enforcement information;
- that the information comes from a confidential source; and
- that the information could possibly reveal the identity of the source.

In order for the source to be considered a "confidential" source, there must be evidence that the information was provided to the public body on the basis of an assurance that the identity of the source of the information would remain confidential (see *IPC Orders 99-010* and *2000-027*).

The assurance of confidentiality may be explicit, for example, stated in a written document, or it may be implied, as in cases where a person supplying the information would do so with a reasonable expectation it would remain confidential.

If information is supplied by an official or employee of a public body as part of his or her job duties, the Commissioner has said that this person cannot be considered a confidential source. For example, an employee providing information to the Workers' Compensation Board was found not to be a confidential source for the purposes of this provision (*IPC Order 99-010*).

The crux of this exception is whether the information may reveal the identity of the confidential source (see *IPC Order 2000-027*). The information may not be in a record created for law enforcement purposes. It may not even refer specifically to the confidential source. If the public body could establish that the information could reasonably reveal the confidential source, the public body could rely on this exception to withhold the information (see *IPC Order 96-019*).

Criminal intelligence

Section 20(1)(e) enables a public body to refuse to disclose one of the most sensitive types of law enforcement information, criminal intelligence.

"**Criminal intelligence**" is information compiled to anticipate, prevent or monitor possible criminal activity. In order to qualify for this exception, the information must:

- have a reasonable connection with the detection, prevention or suppression of organized crime, or
- concern serious and repetitive criminal activities.

Often intelligence is collected for the purpose of law enforcement activities that do not concern organized crime or serious and repetitive crimes. This intelligence information may fall within other exceptions to disclosure, such as the exceptions relating to confidential sources of law enforcement information (**section 20(1)(d)**), investigative techniques (**section (20(1)(c)**) and ongoing or unsolved investigations (**section 20(1)(f)**).

Since intelligence information is often sensitive, it is important to consult with the author of the record, if possible, to determine whether the information meets the criteria for this exception. If so, it is a good idea to label the record as criminal intelligence when it is created and to separate this information from other information in the record.

This provision has not been discussed by the Commissioner to date.

Ongoing or unsolved investigations

Section 20(1)(f) allows a public body to refuse to disclose information if disclosure could reasonably be expected to interfere with or harm an ongoing or an unsolved law enforcement investigation.

A public body could rely on this exception to withhold information if disclosure would "interfere" with an ongoing or unsolved investigation. Disclosure would "interfere" with an investigation if it were to hamper, hinder, or disrupt the investigation. The investigation must be in progress.

With respect to proving harm, a public body would have to meet the harms test discussed above. (See *IPC Order F2004-023.*)

The exception may apply if disclosure may be harmful to an ongoing or active investigation or in a case where investigative activity has ceased but the crime remains unsolved. For example, the exception may apply to information relating to an unsolved fraud investigation.

In *Order F2005-026,* the Adjudicator found that an investigation was "ongoing" where the public body had not yet decided whether to seek a prosecution. The reasonable likelihood that the applicant would use the records in order to alter statements made during the investigation was grounds for withholding the records under **section 20(1)(f)**.

An investigation is still ongoing when the Crown has the files and is considering whether to proceed with charges. At any point during the Crown's assessment, it may ask the public body to gather further evidence (*IPC Order F2004-023*).

Disclosure of information that would indicate that a law enforcement investigation is in progress may be harmful to the investigation. See the discussion below on refusing to confirm or deny the existence of a record under **section 12**.

Prosecutorial discretion

Section 20(1)(g) permits a public body to refuse to disclose information relating to or used in the exercise of prosecutorial discretion.

The exercise of prosecutorial discretion applies to offences under the *Criminal Code of Canada* or any other enactment of Canada or Alberta under which the Attorney General of Alberta may initiate and conduct a prosecution. A prosecutor's discretion arises from the Attorney General on whose behalf the Crown Prosecutors act.

"**Exercise of prosecutorial discretion**" is not defined in the FOIP Act, but the Commissioner's Office has referred to the definition of "prosecutorial discretion" from the British Columbia FOIP Act and case law to determine the meaning of this phrase. (See *IPC Orders 2001-011, 2001-030, 2001-031* and *F2006-005*.)

The B.C. Act defines the exercise of prosecutorial discretion as involving the following activities:

- approving or not approving a prosecution,
- staying a proceeding,
- preparing for a hearing or trial,
- conducting a hearing or trial,
- taking a position on sentence, or
- initiating an appeal.

In *Krieger v. Law Society of Alberta* [2002] 3 S.C.R. 372, the Supreme Court of Canada determined that the exercise of prosecutorial discretion includes the following core elements:

- the discretion whether to bring the prosecution of a charge laid by police,
- the discretion to enter a stay of proceedings in either a private or public prosecution,
- the discretion to accept a guilty plea to a lesser charge,
- the discretion to withdraw from criminal proceedings altogether, and
- the discretion to take control of a private prosecution.

The Court noted that what is common to the various elements of prosecutorial discretion is that they involve the ultimate decision as to *whether* a prosecution should be brought, continued or ceased, and *what* the prosecution ought to be for; in other words, the nature and extent of the prosecution and the Attorney General's participation in it.

Section 20(1)(g) supports the broad policy principles that the exercise of prosecutorial discretion is critically important to the justice system and that prosecutors must be protected from outside influences when deciding whether or not to proceed with a prosecution. (See *IPC Orders F2001-011, F2006-005,* and *F2008-007*.)

In applying this discretionary exception to disclosure, a public body must consider the purpose of **section 20(1)(g)** and whether withholding the records or information in question would meet those purposes in the circumstances of the particular case. The public body must also provide evidence of the factors it considered when applying the exception (*IPC Order F2006-005*).

Many records relating to the exercise of prosecutorial discretion will be in the custody or under the control of Alberta Justice. However, copies of records or notes recording information about the exercise of prosecutorial discretion may be in the files of other public bodies.

The fact that information is in a prosecutor's file does not necessarily mean that **section 20(1)(g)** applies to the information. The substance, not location, of the information is determinative of the matter (*IPC Order F2007-021*).

The exception for prosecutorial discretion is time-sensitive. Information that has been in existence for ten years or more cannot be withheld under this exception (**section 20(2)**). The Commissioner has stated that **section 20(1)(g)** is still relevant where a case has been closed and the 10-year limit has not expired (*IPC Order F2004-030*).

Section 20(6) permits a public body, after the completion of a police investigation, to disclose reasons for a decision not to prosecute to particular parties or to the public under specified circumstances. Disclosure of the reasons not to prosecute would likely reveal some information used in the exercise of prosecutorial discretion.

Section 20(6)(a) allows the reasons to be disclosed to a person who knew of and was significantly interested in the investigation, including a victim or a relative or friend of a victim.

Section 20(6)(b) allows broader disclosure of the reasons to any member of the public, if the fact of the investigation was made public.

Section 20(6) does not provide for the disclosure of records, only reasons for the decision not to prosecute. The public body may be required to create a record for the purpose of providing reasons under this provision.

Right to a fair trial or impartial adjudication

Section 20(1)(h) allows a public body to refuse to disclose information if the disclosure may

deprive a person of the right to a fair trial or impartial adjudication.

For example, this could be information that may influence the atmosphere or opinion of the adjudicator, jury or judge at a trial or hearing. Interference with this right is serious, as the right to a fair trial and impartial adjudication is found in the *Charter of Rights and Freedoms.*

This provision has not been discussed by the Commissioner to date.

Record confiscated by a peace officer

Section 20(1)(i) allows a public body to refuse to disclose information that may reveal a record that has been confiscated from a person by a peace officer in accordance with a law.

This exception requires the public body to prove the following.

- That the information would reveal a record. This could be the record itself that was confiscated or a document that makes reference to or reveals the existence of a record that was confiscated.
- That the record was confiscated by a peace officer. "Peace officer" is defined in section 1(j) of the *Police Act* to mean "a person employed for the purposes of preserving and maintaining the public peace." Other laws, such as the *Corrections Act* (section 10), the *Occupational Health and Safety Act* (section 1(w)) and the *Peace Officer Act* (section 1(f)), set out what "peace officer" means in relation to those laws.
- That the record was confiscated in accordance with a law. The confiscation or seizure powers should be established in a statute or regulation.

This provision has not been discussed by the Commissioner to date.

Information that may facilitate escape

Section 20(1)(j) permits a public body to refuse to disclose information that could reasonably be expected to facilitate the escape from custody of an individual who is being lawfully detained.

An Adjudicator stated that **section 20(1)(j)**, by its nature, is a provision that requires speculation as to the consequences of releasing information. The public body bears the burden of providing cogent evidence to establish a reasonable expectation that disclosure of the information could facilitate an escape from custody. In this case, there was no evidence that the disclosure of a training video relating to the canine unit could facilitate an escape (*IPC Order F2007-005*).

A similar exception in the Ontario FOIP Act is discussed in *Ontario Order P-597*. In that Order the Commissioner upheld the decision to withhold construction plans, including drawings for new windows for a correctional facility, the materials to be used in construction, a list of the type of construction work required, and a general description of the facility's grounds. The Commissioner found that disclosure of records containing this type of information could assist in an escape.

Facilitate the commission of an unlawful act

Section 20(1)(k) allows a public body to refuse to disclose information that could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of crime.

A public body cannot rely on bare assertions that serious consequences will occur if the information is disclosed. The public body must be able to demonstrate how or why the disclosure of the information *at issue* could reasonably be expected to facilitate the commission of an unlawful act or hamper the control of crime. The Commissioner may also examine whether, on the face of the records, there is a reasonable possibility that disclosure of the information would result in the alleged consequence (*IPC Order F2004-032*).

In *Order F2007-005,* the Adjudicator found that the police canine unit could become less effective in apprehending suspects if some of the information in a training video was disclosed to the public. This could hamper the control of crime. However, not all of the training video fell into this category; the introductory and concluding segments of the video containing historical and general information about the unit were to be disclosed.

Reveal technical information about weapons

Section 20(1)(l) allows a public body to refuse to disclose information to an applicant that could reasonably be expected to reveal technical information relating to weapons or potential weapons.

This provision has not been discussed by the Commissioner to date.

Harm the security of any property or system

Section 20(1)(m) allows a public body to refuse to disclose information if the disclosure may reasonably be expected to harm the security of any property or system. This includes security with respect to buildings, vehicles, computer systems, and communication systems.

A public body must meet the requirements of the harms test as discussed above (*IPC Order F2004-032*).

Section 20(1)(m) has been applied to withhold records where their disclosure could be expected to harm the security of communication systems and codes used by the Calgary Police Service in relation to its law enforcement records (*IPC Order F2005-001*). The provision did not apply to a chapter of a police procedural manual where the information relating to the execution of search warrants was common knowledge (*IPC Order F2004-032*).

Reveal information in a correctional record

Section 20(1)(n) allows a public body to refuse to disclose information if the disclosure may reasonably be expected to reveal information in a correctional record supplied, explicitly or implicitly, in confidence.

A "**correctional record**" refers to information in a record created by or for a correctional authority concerning an individual in the custody or under the supervision of correctional authorities or their agents, either in a correctional institution or in the community. A public body may refuse to disclose any information that would *reveal* information supplied in confidence.

This may include information compiled by correctional authorities if the information would reveal the confidential information.

This exception to disclosure has been applied to withhold handwritten client contact records and case notes prepared by a probation officer (*IPC Order 96-004*).

Disclosure may result in civil liability

Section 20(3)(a) gives a public body the discretion to refuse to disclose information in a law enforcement record if the disclosure could reasonably be expected to expose the author of the record, or an individual who has been quoted or paraphrased in the record, to civil liability.

This exception requires that the information be in a "law enforcement" record. The definition of "law enforcement" as discussed above applies. (See *IPC Order 2001-027*.)

Since what may reasonably expose someone to civil liability involves specialized legal knowledge, it may be necessary for a public body to consult legal counsel to ensure the information meets the criteria for this exception. A public body must show to the Commissioner the connection between the disclosure of the information and exposure to civil liability (*IPC Order 2001-027*).

Section 20(3)(b) allows a public body to refuse to disclose information about the history, supervision, or release of an individual who is under the control or supervision of a correctional authority, if the disclosure could reasonably be expected to harm the proper custody or supervision of that person.

The first part of the exception requires that the information be about a person under the control or supervision of a "correctional authority." The term "correctional authority" has not been considered by the Commissioner. However, what constitutes a "correctional institution" in other legislation may provide guidance on what may be considered as a "correctional authority" under the Act. "Correctional institution" is defined in the *Corrections Act* (section 1(1)(b)).

The second part of the exception requires that the public body prove "harm." This may require a public body to meet the harms test described above.

When the exceptions in sections 20(1) and 20(3) do not apply

Section 20(5) provides for specific circumstances in which the exceptions for harm to law enforcement do not apply.

Section 20(5) states that the law enforcement exceptions in **section 20(1)** and **section 20(3)** do not apply to:

- a report prepared in the course of a routine inspection by an agency that is authorized to enforce compliance with an Act of Alberta, or
- a report, including statistical analysis, on the degree of success achieved in a law enforcement program unless disclosure of the report could reasonably be expected to interfere or harm matters referred to in **section 20(1)** or **(3)**.

Disclosure is an offence under a federal Act

Section 20(4) is a mandatory ("must") exception. A public body must refuse to disclose information if

- the information is in a law enforcement record, and
- the disclosure would be an offence under an Act of Canada.

The first requirement of the exception is that the information is contained in a "law enforcement record." The definition of "law enforcement" discussed above applies here.

The second requirement is that a federal statute prohibits the disclosure and makes it an offence to disclose the information. For example, the *Youth Criminal Justice Act* imposes serious limits as to who can view these records and under what circumstances.

In circumstances where the federal statute prevents the Commissioner from ordering the production and review of the documents, the Commissioner will require the public body to produce an affidavit. The requirements of such an affidavit are discussed in *IPC Order 96-015.*

Unreasonable invasion of personal privacy

Section 17 is a mandatory exception. A public body must refuse to disclose personal information if it would be an unreasonable invasion of the personal privacy of a third party to disclose the information.

Section 17(4)(b) establishes a presumption regarding personal information in a law enforcement record:

17(4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if

(b) the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation.

The definition of "law enforcement" in **section 1(h)** applies to this exception. This means that, in the case of an investigation, **section 17(4)(b)** applies only if the information relates to an investigation that leads or could lead to a penalty or sanction under a statute or regulation *(IPC Order 2001-027*).

For example, in *Order 2001-001,* the Assistant Commissioner found that certain investigations under the *Child Welfare Act* resulted in law enforcement records and that disclosure of such records was presumed to be an unreasonable invasion of privacy. At the same time, he noted that not all child welfare records would be considered law enforcement records under the FOIP Act.

Section 17(4)(b) also applies to the complaint leading to the investigation.

In *Order F2003-005*, the Adjudicator found that a Campus Security Report and a complaint to the Alberta Human Rights and Citizenship Commission were both law enforcement records to which the presumption in **section 17(4)(b)** applied.

The public body is required to consider all relevant circumstances, including the circumstances listed in **section 17(5)**, before coming to a final decision under **section 17(1)**.

Section 17 is a mandatory exception; if the Commissioner finds that the exception applies, he will apply it even in cases where the public body has not applied the exception.

Harm to individual or public safety

Information found in records relating to law enforcement is often sensitive, even in cases where the information does not meet the definition of "law enforcement" under the FOIP Act. Public bodies may also need to consider whether the Act's exception for disclosure harmful to individual or public safety may apply to information these circumstances.

Section 18 allows a public body to refuse to disclose information to an applicant, including the applicant's own personal information, if disclosure could reasonably be expected to:

- threaten anyone else's safety or mental or physical health (**section 18(1)(a)**),
- interfere with public safety (**section 18(1)(b)**),
- result in immediate and grave harm to the applicant's safety or health, in the opinion of a health professional or expert (**section 18(2)**), or

if disclosure would reveal the identity of an individual who has provided information to the public body in confidence about a threat to an individual's safety or mental or physical health (**section 18(3)**).

The application of **section 18** calls for a line-by-line analysis to determine which, if any, portions of the records could reasonably be expected to be a threat to the safety of others, if disclosed. Only in very rare cases will this exception to disclosure apply to an entire record (*IPC Order F2004-029*).

Section 18(1)(a) requires the application of the same criteria as in the harms test:

- there must be a causal connection between the disclosure and the anticipated harm,
- the harm must constitute "damage" or "detriment" and not mere inconvenience, and
- there must be a reasonable expectation that the harm will occur. (*See IPC Orders 99-009* and *F2004-032*.)

The application of **section 18(1)(a)** to law enforcement records was considered in *Order F2003-010*. In that case, the Adjudicator upheld the decision of the Edmonton Police Service to withhold records concerning a complaint of elder abuse against the applicant. In *Order F2004-032,* the public body failed to show how the disclosure of a chapter of a police manual relating to the execution of search warrants would threaten the safety of its officers or the general public. Much of the information was either common knowledge or common sense.

Local public body confidences – law enforcement matters

Section 23(1)(b) provides that a local public body may refuse to disclose information if

- disclosure of the information could reasonably be expected to reveal the substance of deliberations of a meeting,
- the meeting is a meeting of the local public body's elected officials or its governing body or a committee of its governing body, and
- the local public body is authorized to hold the meeting in the absence of the public.

Section 18(1)(e) of the FOIP Regulation provides that a local public body that does not have a statute or regulation that addresses *in camera* meetings may rely on this exception to disclosure if the subject-matter being considered concerns, among others things, a law enforcement matter. The Act's definition of law enforcement applies.

The application of **section 23(1)(b)** of the Act in conjunction with **section 18(1)(e)** of the Regulation was considered in relation to the minutes of several meetings held by the Edmonton Police Commission in *IPC Order 2001-040*.

Harm to intergovernmental relations – law enforcement agencies

Section 21(1) provides that a public body may refuse to disclose information that could reasonably be expected to

- harm relations between the Government of Alberta or its agencies and any of the listed government bodies or governmental organizations, or their agencies (**section 21(1)(a)**), or
- reveal information supplied explicitly or implicitly in confidence by any of the above (**section 21(1)(b)**).

This exception may apply to information related to law enforcement that is provided to a public body by an agency of another government. For example, countries share personal information under the *Convention on the Civil Aspects of International Child Abduction*. A public body could refuse to disclose information to an applicant if the disclosure could reasonably be expected to reveal confidential information regarding child abduction that was supplied by another government.

The requirement of harm exists in **section 21(1)(a)**, but not in **section 21(1)(b)** (*IPC Order F2004-018*).

Section 21(2) states that the information to which **section 21(1)(a)** may apply may be disclosed only with the consent of the Minister in consultation with Executive Council.

Section 21(3) states that information to which **section 21(1)(b)** may apply may be disclosed only with the consent of the body that supplied the information.

The application of this exception was considered in *Order 2001-037*. In that case, the information in question was obtained from the Canshare database, which was developed to facilitate the enforcement of Canadian consumer legislation. The Adjudicator decided that disclosure of the information would have been a violation of the agreement governing the database and would undermine the legislative policy underlying **section 20(1)(b)** of the FOIP Act, which is to protect the free flow of information between governments.

In *Order F2004-018*, an off-duty officer of the Edmonton Police Service (EPS) had a verbal exchange with an RCMP officer. The RCMP subsequently sent information about the incident to EPS. The Commissioner found that EPS could withhold the information under **section 21(1)(b)**. The possibility that the information may have to be disclosed during a future disciplinary hearing or criminal prosecution did not affect the fact that the information was initially supplied to EPS in confidence.

Refusal to confirm or deny existence of a record

If a public body does not disclose a record in whole or in part in response to an access request, the applicant is entitled under **section 12(1)(c)(i)** to be told the reason for the refusal and the provision of the Act on which the refusal is based.

However, **section 12(2)(a)** provides that a public body may refuse to confirm or deny the existence of a record if disclosure of information in the record would be:

- harmful to individual or public safety (under **section 18**), or
- harmful to law enforcement (under **section 20**).

Section 12(2)(b) provides that a public body may refuse to confirm or deny the existence of a record containing personal information about a third party if disclosing the existence of the information would be an unreasonable invasion of a third party's personal privacy (under **section 17**).

A public body generally cannot rely on either provision of **section 12(2)** without first conducting a search to determine whether responsive records exist. The public body should be prepared to provide those records to the Commissioner for review, if requested to do so (*IPC Order 98-009*). There may be circumstances where the application of **section 12(2)** is so clear that a search may not be warranted.

With respect to **section 12(2)(b)**, the public body must determine whether the disclosure of the existence of the record would be an unreasonable invasion of a third party's privacy. **Section 17** may act as a guide

to public bodies for determining whether there would be an unreasonable invasion of personal privacy. However, the focus of the analysis for purposes of **section 12(2)(b)** must be on whether the disclosure of the existence of the information, rather than whether the disclosure of the information itself, would constitute an unreasonable invasion of a third party's personal privacy. (See *IPC Orders 98-009* and *2000-004*.)

In *Order F2007-003*, the Adjudicator found that revealing whether or not the police made or kept records about a matter in which they were publicly known to have investigated would not be an unreasonable invasion of the personal privacy of persons who were also known to be involved in the matter.

Earlier decisions (e.g. *IPC Order 2000-016*) have held that, in order to apply **section 12(2)(a)**, a public body need only establish that a record contained information described in **section 18** or **20**. The public body did not have to take the additional step, as it does in **section 12(2)(b)**, of establishing that disclosure of the existence of the information would result in the harm referred to in **section 18** or **20**.

This position has been overturned by *Orders F2006-012* and *F2006-013* (October 10, 2006). The Commissioner stated that in order to rely on **section 12(2)(a)**, a public body must first consider what interest would be protected by withholding the record under **section 18** or **20**, and then consider whether refusing to say if such information exists would promote or protect the same interest. In other words, the public body must be able to show that disclosure of whether the information exists or not would result in one of the negative consequences in **section 18** or **20**. (See also *IPC Orders F2006-020, F2006-011*, and *F2006-015*.)

Section 12(2) significantly interferes with an applicant's access rights under the Act. If an applicant requests a review of an access decision by the public body, the public body will be required to provide specific and compelling evidence to the Commissioner regarding its reasons for using this provision. (See *IPC Orders 98-009* and *F2006-013*.)

If a public body refuses to confirm or deny the existence of the records requested by an applicant, the Commissioner is also prohibited by **section 59(3)(b**) from disclosing whether the requested information exists. This prohibition extends to the writing of his decision. In these circumstances, parts of a public body's submissions may be made *in camera* and the Commissioner may write an addendum to the Order which will include his reasons on the *in camera* information. The addendum will be provided only to the public body, and to the court, under seal, when a judicial review application is made. (See *IPC Orders F2006-012* and *F2006-013*.)

DISCLOSURE IN THE PUBLIC INTEREST

Information that concerns law enforcement or information found in a law enforcement record often relates to issues of health and safety or matters of public interest.

Section 32(1) is a mandatory provision that directs a public body to disclose, whether or not an access request has been made,

- information about a risk of significant harm to the environment or to the health or safety of the public, of the affected group of people, of the person or of the applicant (**section 32(1)(a)**), or
- information the disclosure of which is, for any other reason, clearly in the public interest (**section 32(1)(b)**).

The information can be disclosed to the public, to an affected group of people, to any person, or to an applicant, depending on what kind of information it is and whom it affects.

This section is an "override" provision, meaning that, if the criteria for **section 32(1)** are met, the requirement to disclose the information applies despite any other provision in the Act (**section 32(2)**). It is therefore important that the public body ensures that the information falls squarely within the criteria set out in **section 32(1)**. These criteria should be interpreted narrowly. (See *IPC Order 96-011*).

With respect to **section 32(1)(a)**, a public body will be required to provide evidence that its decision is reasonable (see *IPC Orders 96-011* and *98-017*).

The disclosure should be made in the least intrusive manner possible and the information released should be proportionate to the risk (see *IPC Investigation Report 98-IR-011*).

With respect to **section 32(1)(b)**, the Commissioner has indicated that "clearly in the public interest" means the matter must be of "compelling public interest" (see *IPC Orders 96-011, 96-014, 2000-017,* and *2000-023*).

This provision has been used when a violent or dangerous offender is being released from custody. The public or affected group receives a notification of the release by the relevant police service or correctional authority (see *IPC Investigation Report 98-IR-011*). It has also been used by applicants to argue that information should have been released by a public body, even without an access request (see, for example, *IPC Orders 97-009* and *98-017* with respect to information in investigation documents concerning possible environmental contamination).

PRIVACY PROTECTION UNDER PART 2

Part 2 of the FOIP Act controls the manner in which a public body collects, uses and discloses personal information for all purposes, including law enforcement. A public body can collect personal information for the purpose of law enforcement only if the law enforcement activity falls within the definition in **section 1(h**) of the Act. This definition of "law enforcement" is discussed in detail in the Introduction to this Bulletin.

Section 33(a) authorizes a public body to collect personal information if the collection of that information is expressly authorized by an enactment of Alberta or Canada. In many cases public bodies whose mandate includes law enforcement will have specific investigative powers set out in their governing legislation. A public body that collects personal information under **section 33(a)** can collect personal information indirectly (from a person other than the individual the information is about) only if authorized to do so under **section 34(1)**.

Section 33(b) authorizes a public body to collect personal information for the purpose of law enforcement. If a public body is authorized to collect personal information under this provision, it is also authorized to collect the information indirectly under **section 34(1)(g)**.

The Commissioner has stated that the authority for collection under **section 33(b)** ends when a police officer knows, or should know, that there is no longer a law enforcement issue; for example the officer has determined that there is no threat, no crime or no law broken (*IPC Order F2006-002*).

A public body that is authorized to collect personal information indirectly is not required to provide notice with respect to that collection of personal information (**section 34(2)** of the FOIP Act). However, a public body that collects personal information that falls within **section 34(1)(a)** to **(o)** directly from the individual concerned may *choose* to provide notice, especially in cases where doing so would not be likely to compromise the accuracy of the information.

A public body that collects personal information for a law enforcement purpose should not collect excessive amounts of personal information. One of the situations where this is most likely to occur is in the use of surveillance. The Commissioner considered the use of video surveillance for law enforcement purposes in *Investigation Report F2003-IR-005*. This topic is treated in detail in the *Guide to Using Surveillance Cameras in Public Areas*, produced by Access and Privacy, Service Alberta.

Section 39 provides that a public body may use the personal information it has collected only for authorized purposes, including the purpose for which it was originally collected or for a use consistent with that purpose, and for a purpose for which information may be disclosed under the Act's disclosure provisions (especially **section 40**). For example, a public body will contravene **Part 2** of the FOIP Act if its employees access the personal information in the Canadian Police Information Centre (CPIC) system for purposes unrelated to law enforcement. (See *IPC Investigation Report F2005-IR-001*.)

This section of the Bulletin will focus on **section 40** as it relates specifically to law enforcement.

In all cases, the use and disclosure of personal information is limited by **section 39(4)** and **section 40(4)** respectively. These provisions require the

public body to use or disclose personal information only to the extent necessary for the purpose.

Disclosure not an unreasonable invasion of personal privacy

Section 40(1)(b) provides that personal information may be disclosed if the disclosure would not be an unreasonable invasion of a third party's personal privacy under **section 17**. This provision would authorize disclosure of third party personal information found in an identifiable law enforcement record. **Section 17(4)(b)** provides for an exception to the presumption that it is an unreasonable invasion of personal privacy to disclose personal information in a law enforcement record. This presumption does not apply if disclosure of the information is necessary to dispose of the law enforcement matter or to continue an investigation. The public body must still consider all relevant circumstances in reaching a decision under **section 40(1)(b)**.

For example, an occupational health and safety officer may need to disclose some background information about an investigation, including personal information about a third party, to a possible witness. The disclosure may be necessary to obtain a complete and accurate witness statement. In this case, disclosure is unlikely to be considered an unreasonable invasion of the third party's privacy. The disclosure of the third party's personal information should be limited to information necessary for the purposes of the law enforcement investigation.

Disclosure authorized or required by law

In many cases where a public body receives a request from a law enforcement agency for disclosure of personal information, disclosure of the information is authorized by legislation or by a treaty, arrangement or agreement. The FOIP Act permits a public body to disclose the requested information under **section 40(1)(e)** or **(f)**, as applicable.

If disclosure is *required* by law, the public body must disclose the information necessary to respond to the request. There is no conflict in these cases between the FOIP Act ("a public body *may* disclose") and other laws that *compel* disclosure.

In a case where a public body is asked to disclose personal information in accordance with another law, the public body should limit the disclosure to the information described in the applicable law.

A special case of disclosure authorized by an enactment of Alberta is disclosure of reasons not to prosecute which is authorized by **section 20(6)** of the FOIP Act. This provision permits a public body, after the completion of a police investigation, to disclose reasons for a decision not to prosecute to particular parties. (See page 8 for a more detailed discussion of this provision.)

Disclosure to assist in an investigation

Section 40(1)(q) authorizes disclosure of personal information by a public body to another public body or a law enforcement agency in Canada to assist in an investigation

- undertaken with a view to a law enforcement proceeding, or
- from which a law enforcement proceeding is likely to result.

When disclosing personal information under **section 40(1)(q)**, the releasing public body should satisfy itself that

- the requesting party is a "public body" within the meaning of **section 1(1)(p)** or is a "law enforcement agency,"
- there is a law enforcement investigation and that the investigation has been undertaken with a view to a law enforcement proceeding as defined in **section 1(h)** (i.e. a proceeding that can result in a penalty or sanction under a statute or regulation), and
- the requesting public body or law enforcement agency can provide the legal authority for the law enforcement activity (a form for this purpose is included in Appendix 5 in *FOIP Guidelines and Practices*).

The term "**law enforcement agency**" is not defined in the FOIP Act, although the definition of "law enforcement" applies when considering whether an agency is responsible for law enforcement. Some

examples of law enforcement agencies that are not public bodies are the RCMP, First Nations' police services, Canada Revenue Agency and the federal Superintendent of Financial Institutions.

Disclosure by a law enforcement agency

Section 40(1)(r) permits a public body to disclose personal information if the public body is a law enforcement agency and the information is disclosed

- to another law enforcement agency in Canada (**section 40(1)(r)(i)**), or
- to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority (**section 40(1)(r)(ii)**).

There is no list of public bodies that are also "law enforcement agencies." In *Order 96-007*, the Commissioner examined whether a branch of Alberta Justice, the Edmonton Remand Centre, was a law enforcement agency. The Commissioner stated that since Alberta Justice is involved in law enforcement, it was a "law enforcement agency" and any of its various branches are considered law enforcement agencies.

In *Order F2006-018*, the Workers' Compensation Board (WCB) was found to be a law enforcement agency in relation to its investigation of the veracity of an individual's disability claim. The municipal district, to which the WCB disclosed the individual's personal information in order to obtain a legal land description, was also a law enforcement agency. This is because the division of the municipal district responsible for protective services and highway patrol is engaged in law enforcement. The disclosure of personal information was permitted under **section 40(1)(r)(i)**.

Section 40(1)(r)(ii) permits disclosure to a foreign law enforcement agency in accordance with an arrangement, written agreement, treaty, or legislative authority. This would include, for example, a treaty, convention or other international agreement under the federal *Mutual Legal Assistance in Criminal Matters Act.*

The releasing public body should satisfy itself that the foreign body or the extra-provincial agency is a "law enforcement agency." If the law enforcement agency is foreign, the releasing public body must ensure that the disclosure is made in accordance with a formal written arrangement. This may require the releasing public body to contact other government bodies, such as the federal Department of Justice, Department of Foreign Affairs or the RCMP, for example, to verify that the information sharing is permitted by the appropriate arrangement, agreement or treaty.

Section 40(1)(r) does not require that the two agencies be involved in the same law enforcement matter, but it is implied that the disclosure will be for a legitimate law enforcement purpose (*IPC Order F2006-018*).

COLLECTION OF INFORMATION FROM THE PRIVATE SECTOR

Since January 2004, privacy legislation has applied to most organizations in the private sector.

Alberta's *Personal Information Protection Act* (PIPA) applies to provincially regulated organizations conducting transactions within Alberta. PIPA (section 20(c)) permits an organization to disclose personal information to a public body that is authorized to collect that information. PIPA does not affect the ability of law enforcement agencies that are subject to the FOIP Act to operate within Alberta.

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to federally regulated organizations operating within Alberta and to organizations conducting transactions that involve the transfer of personal information across provincial boundaries. PIPEDA (section 7(3)(c.1)) permits an organization to disclose personal information to a government body that

- makes a request for the information,
- identifies its lawful authority to obtain the information, and
- indicates that the information relates to national security, law enforcement or the administration of any law of Canada or a province.

For further information about PIPEDA, see the federal Privacy Commissioner's website at www.privcom.gc.ca.

Some private sector organizations may be uncertain as to whether they can disclose personal information to law enforcement agencies for the purposes of

investigations. To assist law enforcement agencies in collecting personal information from private sector organizations that are subject to either PIPA or PIPEDA, Access and Privacy, Service Alberta has produced the following guidelines: *Requesting Personal Information from the Private Sector – Forms and Guidelines for Law Enforcement Agencies.*

PRACTICAL TIPS ON MANAGING LAW ENFORCEMENT INFORMATION

Creating law enforcement records

- A general rule in the creation of any record by a public body is that it should contain professional language and observations. This is particularly important with law enforcement records, which are commonly requested by parties involved in a dispute.
- As much as possible, separate the personal information of different individuals. For example, in incident reports or an investigative officer's notes, the information received from an interview of one witness should be segregated from the information received from another witness.
- Identify information that may qualify for a law enforcement exception. Document reasons for the identification. Evaluation and classification at the time the record is created may assist a public body evaluating information that is responsive to an access request some time after the creation of the record. This information may also assist other public bodies if the records are shared.

For example, criminal intelligence information and information received from a confidential source should be identified. It should be made clear when information is provided in confidence. Keep in mind, however, that labelling the information does not automatically entitle the information to an exception; the public body processing the request is responsible for evaluating whether the information meets the requirements of an exception, and for exercising its discretion appropriately.

Sharing law enforcement records with other public bodies

Law enforcement records may be created by one public body and disclosed to another public body, under the provisions of **section 40**. If the law enforcement records are in the custody of the receiving public body and are responsive to an access request under **Part 1** or a request for disclosure under **Part 2**, it is often difficult for the public body processing the request to know the context or circumstances under which the documents were originally created.

Indicating on the record itself that it is or contains law enforcement information within the meaning of the Act, and providing contact information for a person able to answer questions about the record, will assist the public body responding to the request for information.

Currency

This Bulletin takes into consideration decisions issued by the Office of the Information and Privacy Commissioner of Alberta up to December 31, 2008.

Purpose

FOIP Bulletins are intended to provide FOIP Coordinators with more detailed information for interpreting the *Freedom of Information and Protection of Privacy Act*. They supply information concerning procedures and practices to assist in the effective and consistent implementation of the FOIP Act across public bodies. FOIP Bulletins are not a substitute for legal advice.

Further Information

Access and Privacy
Service Alberta
3rd Fl., 10155 – 102 Street
Edmonton, Alberta T5J 4L4
Phone: 780-427-5848
Website: foip.alberta.ca