### **ALBERTA**

# OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

# **ORDER F2014-06**

January 30, 2014

# ALBERTA JUSTICE AND SOLICITOR GENERAL

Case File Number F6044

Office URL: www.oipc.ab.ca

**Summary:** The Criminal Trial Lawyers Association, (the Applicant), made a request for access to information under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act) to Alberta Justice and Solicitor General (the Public Body). The Applicant stated that to its knowledge, a member of a police service, whom it named, had been involved in a sexual relationship with an informant, that the police member was suspended from his duties and that he subsequently committed suicide. The Applicant stated that it was also aware that the Alberta Serious Incident Response Team (ASIRT) had investigated the matter. The Applicant stated that it was seeking a copy of the ASIRT final report. Finally, the Applicant stated that it was seeking records that would contain information revealing whether the police member it named had taken part in any prosecutions and whether Crown prosecutors had alerted accused persons in such cases of the police member's relationship with the informant.

The Public Body responded to the Applicant's access request on November 22, 2011. The Public Body stated that if the records existed, confirming their existence would be an unreasonable invasion of a third party's personal privacy within the terms of section 17 of the FOIP Act. The Public Body also noted that if the records existed, they would contain information subject to sections 18 and 20 of the FOIP Act. For both reasons, the Public Body declined to confirm or deny the existence of responsive records under section 12(2) of the FOIP Act.

The Adjudicator found that confirming the existence of responsive records, if such existed, would disclose personal information of the police member who was the subject of the Applicant's allegations. The Adjudicator found that it would be an unreasonable invasion of the police member's personal privacy to disclose the existence of any responsive records. The Adjudicator confirmed the Public Body's decision to apply section 12(2)(b) of the FOIP Act.

**Statutes Cited: AB:** Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25, ss. 1, 6, 12, 17, 18, 20, 68, 72 The Police Act, R.S.A. 2000, c. P-17, s. 46.1

**Authorities Cited: AB:** Orders 2000-012, F2006-012, F2010-010, F2011-001, F2012-24

Cases Cited: University of Alberta v. Pylypiuk, 2002 ABQB 22

## I. BACKGROUND

[para 1] On October 11, 2011, the Criminal Trial Lawyers' Association (the Applicant) made a request for access to information under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act) to Alberta Justice and Solicitor General (the Public Body). The Applicant stated that to its knowledge, a member of a police service, whom it named, had been involved in a sexual relationship with an informant, that the police member was suspended from his duties, and that the member subsequently committed suicide. The Applicant stated that it was also aware that the Alberta Serious Incident Response Team (ASIRT) had investigated the matter and the Applicant was seeking a copy of the ASIRT final report. Finally, the Applicant stated that it was seeking records that would contain information revealing whether the police member it named had taken part in any prosecutions and whether Crown prosecutors had alerted accused persons in any such cases of the police member's relationship with the informant.

[para 2] The Public Body responded to the Applicant's access request on November 22, 2011. The Public Body stated that if the records existed, confirming their existence would be an unreasonable invasion of a third party's personal privacy within the terms of section 17 of the FOIP Act if the records existed. The Public Body also noted that if the records existed, they would contain information subject to sections 18 and 20 of the FOIP Act. For both reasons, the Public Body declined to confirm or deny the existence of responsive records under section 12(2) of the FOIP Act.

[para 3] The Applicant requested review by the Commissioner of the Public Body's response. The Commissioner authorized a mediator to investigate and attempt to settle the matter under section 68 of the FOIP Act. As mediation was unsuccessful, the matter was scheduled for a written inquiry.

## II. ISSUE

Issue A: Did the Public Body properly refuse to confirm or deny the existence of a record as authorized by section 12(2) of the Act (contents of response)?

#### III. DISCUSSION OF ISSUE

# Issue A: Did the Public Body properly refuse to confirm or deny the existence of a record as authorized by section 12(2) of the Act (contents of response)?

- [para 4] Section 12 of the FOIP Act sets out the kinds of information a public body's response to an applicant must contain. This provision states:
  - 12(1) In a response under section 11, the applicant must be told
    - a) whether access to the record or part of it is granted or refused,
    - (b) if access to the record or part of it is granted, where, when and how access will be given, and
    - (c) if access to the record or to part of it is refused,
      - (i) the reasons for the refusal and the provision of this Act on which the refusal is based,
      - (ii) the name, title, business address and business telephone number of an officer or employee of the public body who can answer the applicant's questions about the refusal, and
      - (iii) that the applicant may ask for a review of that decision by the Commissioner or an adjudicator, as the case may be.
  - (2) Despite subsection (1)(c)(i), the head of a public body may, in a response, refuse to confirm or deny the existence of
    - (a) a record containing information described in section 18 or 20, or
    - (b) a record containing personal information about a third party if disclosing the existence of the information would be an unreasonable invasion of the third party's personal privacy.
- [para 5] Section 12(2) creates an exception to the requirement created by section 12(1)(c)(i) that a public body provide reasons for refusing to disclose information and to cite the provision on which a refusal is based. Section 12(2)(a) may be applied when the record contains information described in sections 18 or 20. Section 12(2)(b) may be applied when the requested record contains personal information and disclosing the existence of the information would in itself be an unreasonable invasion of personal privacy.
- [para 6] As noted in the background above, the Public Body argues that both sections 12(2)(a) and (b) apply in this case. I turn now to the question of whether section

12(2)(a) authorizes the Public Body to refuse to confirm or deny the existence of responsive records.

Section 12(2)(a)

[para 7] Cited above, section 12(2)(a) allows a public body to refuse to confirm or deny the existence of a record containing information described in section 18 or 20 of the FOIP Act. The Public Body makes the following argument in support of its application of this provision:

Under section 12(2)(a) of the Act, a public body may refuse to confirm or deny the existence of a record, [...], if the record contains information described in sections 18 or 20 of the Act[...]

[...]

Section 18(1) (Disclosure harmful to individual or public safety) of the Act reads, in part, as follows:

18(1) The head of a public body may refuse to disclose to an applicant information, including personal information about the applicant, if the disclosure could reasonably be expected to

(a) threaten anyone else's safety or mental or physical health[...]

Section 12(2)(a) does not require the Public Body to establish the existence of a "threat" by applying the Harms test. It requires the Public Body to determine if a record contains information that if disclosed, would "threaten anyone else's safety or mental or physical health." Section 12(2)(a) contemplates what is being requested and would it be reasonable to conclude that the disclosure of any records, if they exist, be reasonably expected to harm any identified third parties as outlined in section 18(1)(a) of the Act.

The Applicant has requested "a copy of the final report of ASIRT ... and information provided by this informant" pertaining to allegations "that [a detective] was in a sexual relationship with an informant..." It is the position of the Public Body, that it is reasonable to conclude that any records, regardless if they exist or not, would contain information as defined in section 18 of the Act.

If the fact scenario alleged by the Applicant were true, which the Public Body neither confirms nor denies, the disclosure of such information, regardless if it exists or not, would place the third party's (i.e. alleged informant reporting on alleged criminal activity) safety, mental or physical health in jeopardy.

Section 20(1) (Disclosure harmful to law enforcement) of the Act reads, in part, as follows:

20(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

(a) harm a law enforcement matter,

[...]

(d) reveal the identity of a confidential source of law enforcement information,

(e) reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities.

[...]

(k) facilitate the commission of an unlawful act or hamper the control of crime [...]

"Law enforcement" is defined under section 1(h) (Definitions) of the Act, as follows:

[(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[...]

Section 12(2)(a) of the Act does not require the Public Body to apply the Harms Test for section 20. It requires a public body to determine if a record may contain information described in section 20. Based on the wording of the Applicant's request which includes an alleged statement that the [police] member was "suspended and told that there would likely be criminal charges", if records do exist, which the Public Body neither confirms nor denies, it is reasonable to believe that there is a law enforcement investigation and therefore the records would contain information described in section 20. What section 12(2)(a) contemplates is that based on what information is being requested, would it be reasonable to conclude that the records could impact a law enforcement matter.

It is the position of the Public Body that based on the request itself, it is reasonable to conclude that any records, regardless if they exist or not, which the Public Body neither confirms nor denies, would contain information as defined in section 20.

If the fact scenario alleged by the Applicant were true, which the Public Body neither confirms nor denies, the disclosure of such information, regardless if it exists or not, could reasonably be expected to harm a law enforcement matter, reveal the identity of confidential sources of law enforcement information, reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities, and facilitate the commission of an unlawful act or hamper the control of crime (see sections 20(1)(a), 20(1)(d), 20(1)(e), and 20(1)(k)).

[para 8] While it is not strictly necessary for me to address the Public Body's submissions in relation to section 12(2)(a), given my conclusion in relation to the application of section 12(2)(b), below, the Public Body's application of this provision requires some comment.

[para 9] I agree with the Public Body that any records responsive to the Applicant's access request would refer to law enforcement matters, given that the access requests contains reference to police disciplinary action and to an ASIRT investigation. Both processes are investigations that could result in penalty or sanction as described by section 1(h) of the FOIP Act. However, I disagree with the position that a public body need only establish that any responsive records would contain information that could reasonably be expected to result in the harm contemplated by section 18 or one of the harmful outcomes set out in section 20(1), before it may rely on section 12(2)(a) to refuse to confirm or deny the existence of a record.

# [para 10] In Order F2006-012, former Commissioner Work commented on the application of section 12(2)(a). He said:

Earlier orders of this Office have said that section 12(2) is to be used having regard to the objects of the Act, including access principles. In my view, in order to rely on section 12(2)(a) to refuse to say whether information exists that falls into a particular subsection of section 18 or 20, the Public Body should first consider what interest would be protected by withholding such information under the particular subsection of section 18 or 20, and then ask whether refusing to say if such information exists would, in the particular case, promote or protect the same interest. A line of Ontario decisions, which includes a decision of the Ontario Court of Appeal, support this interpretation. These cases interpret similar Ontario legislation that restricts the use of the "refuse to confirm or deny" provision to situations where the refusal to say if the information exists protects the same interest as refusal to disclose the information. The Ontario legislation does not impose such a restriction expressly. However, the Office of the Information and Privacy Commissioner has, on many occasions, read in such a restriction, relative to both a provision that permits refusal to confirm or deny whether records exist that would, if disclosed, be an unjustified invasion of personal privacy, as well as in relation to provisions that permit refusal to confirm or deny records the disclosure of which would harm law enforcement matters. For example, in Order P-344, the Assistant Commissioner, in interpreting section 14(3) of the Ontario Freedom of Information and Protection of Privacy Act (which permits refusal to confirm or deny a record where disclosure of the record could cause specified consequences very similar to those listed in section 20 of the Alberta Act), said:

A requester in a section 14(3) situation is in a very different position than other requesters who have been denied access under the Act. By invoking section 14(3), the institution is denying the requester the right to know whether a record exists, even when one does not. This section provides institutions with a significant discretionary power which I feel should be exercised only in rare cases.

In my view, an institution relying on section 14(3) must do more than merely indicate that records of the nature requested, if they exist, would qualify for exemption under sections 14(1) or (2). An institution must provide *detailed and convincing evidence* that disclosure of the mere existence of the requested records would convey information to the requester which could compromise the effectiveness of a law enforcement activity. [emphasis added in original]

The Ontario Court of Appeal recently approved this interpretation (dealing with a refusal to confirm or deny the existence of a report pursuant to the provision relating to unjustified invasion of privacy), and leave to appeal to the Supreme Court of Canada has been denied. The majority said:

The Commissioner's reading ... requires that in order to exercise his discretion to refuse to confirm or deny the report's existence, the Minister must be able to show that

disclosure of its mere existence would itself be an unjustified invasion of personal privacy. The scheme of the Act is designed both to advance public access to information and protection of individual privacy and also to provide the necessary balancing of these purposes. ... [T]he Act itself uses the concept of an unjustified invasion of privacy to strike the balance between access and privacy with respect to personal information contained in a report. The Commissioner's reading ... uses the same concept for the same purpose where the information is the fact of the existence of a report rather than its contents. ... The Commissioner reads the discretion given by the subsection to be constrained in this way in reflection of the Act's fundamental purposes and the balance required to be struck between them. In my view this is a reasonable interpretation ...

This analysis applies equally to section 12(2)(a): whether a specified harm to law enforcement will be caused is the "concept" used to strike the balance between access rights and the goals of law enforcement. This is the approach that has been taken by the Ontario Privacy Commissioner's Office, and I agree with it.

As noted earlier, the Alberta legislation differs somewhat from that in Ontario, in that our section 12(2)(b) (unreasonable invasion of privacy) expressly contains the restriction just discussed, but 12(2)(a) (which refers to information described in sections 18 and 20) does not. Arguably, this could be taken to mean that such a restriction should be applied only to the former and not the latter. However, the result would be that section 12(2)(a) may be relied on only in situations where information is described by the subsections, yet a decision to use it may be made for some completely unknown, unrelated purpose. This is not a sensible result. The sensible purpose for both provisions is that it is to prevent requestors from obtaining information from a request indirectly that they cannot obtain directly. Requestors are denied access to information if access would cause harm to law enforcement, or unreasonable invasion of privacy. They should be denied information as to whether a record exists for the same reason, but not otherwise. Despite the difference in wording between sections 12(2)(a) and 12(2)(b), this restriction makes the same sense for both sections; therefore, in my view, it was intended for both, and I interpret section 20(1)(a) as implicitly containing it. The discretion to refuse to confirm or deny is available only if the condition is met that it is being used to protect the same interest as non-disclosure of information. This interpretation is also in accordance with the general principle in the Act of permitting access subject only to limited and specific exceptions.

- [para 11] I agree with former Commissioner Work's analysis. I would add that in my view, the presence of section 6(2) of the FOIP Act supports the interpretation at which he arrived in Order F2006-012. Section 6(2) states:
  - 6(2) The right of access to a record does not extend to information excepted from disclosure under Division 2 of this Part, but if that information can reasonably be severed from a record, an applicant has a right of access to the remainder of the record.
- [para 12] Section 12(2)(a) does not apply notwithstanding section 6(2). As a result, the duty to sever information that is subject to an exception to disclosure (such as section 18 or 20) and to provide the remaining information to an applicant, remains, despite the application of section 12(2). If a public body could exercise discretion to refuse to confirm or deny the existence of records, simply because they contain information subject to section 18 or 20, even though the information could reasonably be severed from the records, then the right of access to the remaining information granted to an applicant by section 6(2) would be meaningless.

[para 13] If sections 12(2)(a) and 6(2) are not to be read as being in conflict with one another, section 12(2)(a) should be read as permitting a public body to refuse to confirm or deny the existence of a record when information subject to section 18 or 20 cannot be reasonably severed from the record and a response complying with section 12(1)(c)(i) would have the effect of disclosing the information. This interpretation is consistent with that proposed by former Commissioner Work in Order F2006-012.

*Section 18(1)(a)* 

[para 14] The application of section 18(1)(a), to which the Public Body refers in its submissions, depends on there being information in records that could reasonably be expected to threaten anyone else's safety or mental or physical health if the information were disclosed. Section 12(2)(a) does not relax this requirement. Section 12(2)(a) permits a public body to refuse to confirm or deny the existence of a record if the record would contain information subject to section 18(1)(a).

# [para 15] Section 18(1)(a) states:

- 18(1) The head of a public body may refuse to disclose to an applicant information, including personal information about the applicant, if the disclosure could reasonably be expected to
  - (a) threaten anyone else's safety or mental or physical health[...]
- [para 16] The Public Body argues that disclosing the existence of responsive records, if any, would subject the informant referred to in the Applicant's access request (if such a person exists) to harm as contemplated by section 18(1)(a).
- [para 17] For section 18(1)(a) to apply, it must be established, with detailed and convincing evidence, that disclosing particular information could reasonably be expected to threaten the safety or mental or physical health of someone other than an applicant.
- [para 18] For section 12(2)(a) to apply, it must be established that confirming the existence of records would have the effect of disclosing information subject to section 18.
- [para 19] I accept that there may be cases when confirming the existence of a confidential police informant may serve to identify an informant. For example, if a requestor knew sufficient details about a case, being told that there was an informant might be sufficient information to enable the requestor to identify the informant or potential informants. If disclosing information would have the effect of disclosing the identity of a confidential police informant or possible informants, then section 18 would apply to the information. If confirming the existence of a responsive record would also have the effect of disclosing such information, then section 12(2)(a) would apply so that

the head of a public body could exercise discretion to refuse to disclose the existence or non-existence of the records.

[para 20] However, I am unable to find that disclosing the existence of responsive records would in this case serve to identify a confidential police informant. I say this because the circumstances in which an informant is said to have provided information to the police have not been established for the inquiry. As a result, I am unable to find that the identity of an informant would be revealed by disclosing the *existence* of records responsive to the Applicant's access request. The Public Body's submissions do not provide any evidence or explanation as to how confirming whether responsive records exist or not would serve to identify a confidential police informant. Rather, in a scenario where responsive records exist, it would appear that the identity of the informant could be severed from them, and the remaining records provided to the Applicant, as required by section 6(2) of the FOIP Act.

Section 20

[para 21] Sections 20(1)(a), (d), (e), and (k), to which the Public Body also refers, require a reasonable likelihood that disclosure of information could result in the harms set out in these provisions before they may be applied. These provisions state:

20(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

(a) harm a law enforcement matter,

*[...]* 

- (d) reveal the identity of a confidential source of law enforcement information,
- (e) reveal criminal intelligence that has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities,

*[...1* 

- (k) facilitate the commission of an unlawful act or hamper the control of crime [...]
- [para 22] The Public Body's arguments in relation to the application of these provisions are to the effect that if one can presume from the access request that responsive records would contain information that would "impact a law enforcement matter", the requirements of these provisions are met. However, that information could possibly have an effect on a law enforcement matter does not bring the information within the terms of any of the provisions of section 20 that the Public Body has cited or

permit the Public Body to rely on section 12(2)(a) to refuse to confirm or deny the existence of records.

- [para 23] If the Public Body were to confirm the existence of responsive records, and such records existed, then the Public Body would be confirming one or more of the following statements: that a police officer had an affair with an informant; that the police officer was suspended, that the police officer committed suicide, and that ASIRT conducted an investigation into these events.
- [para 24] There is no evidence before me to establish the likelihood that confirming the *existence* of responsive records would harm a law enforcement matter (which the terms of the Applicant's access request indicate would have been concluded in any event), or reveal the identity of a confidential source of law enforcement information, or reveal criminal intelligence or facilitate the commission of an unlawful act or hamper the control of crime.
- [para 25] As I find that it has not been established that confirming the existence of responsive records would reveal information subject to sections 18 or 20, I find that section 12(2)(a) does not authorize the Public Body to refuse to confirm or deny the existence of responsive records.

*Section 12(2)(b)* 

[para 26] Cited above, section 12(2)(b) states:

- 12(2) Despite subsection (1)(c)(i), the head of a public body may, in a response, refuse to confirm or deny the existence of
  - (b) a record containing personal information about a third party if disclosing the existence of the information would be an unreasonable invasion of the third party's personal privacy.

## [para 27] The Public Body argues:

It is the Public Body's position that the disclosure of the existence or non-existence of the requested information would be an unreasonable invasion of third parties' personal privacy. The Public Body neither confirms nor denies whether the fact scenario alleged in the Applicant's access request is correct or whether records responsive to his request exist. However, the Public Body will base its submissions on the fact scenario alleged by the Applicant so that it can discuss its analysis in detail, and so the Applicant will be able to respond.

Based on the fact scenario alleged by the Applicant, the Public Body submits that confirming or denying whether responsive records exist or do not exist would reveal the following personal information about third parties:

- That one third party was a police [officer], had a sexual relationship with an informant, that this resulted in an investigation and his subsequent death; and
- That one third party was an informant, had a sexual relationship with a police officer, that this resulted in an investigation and the police officer's subsequent death.

If the fact scenario alleged by the Applicant is correct in that two individuals were in a sexual relationship that resulted in a police investigation, which the Public Body neither confirms nor denies, the information in the records, if they exist would likely be highly sensitive personal information and disclosure would be an unreasonable invasion of the third parties' personal privacy.

[para 28] The Public Body appears to advance the interpretation that section 12(2)(b) applies if the information present in any responsive records would be highly sensitive. However, this interpretation is not supported by the language of section 12(2)(b). As discussed in Order F2006-012, and as indicated by the language of the provision itself, section 12(2)(b) applies only when disclosing the existence of personal information would in itself be an unreasonable invasion of a third party's personal privacy.

[para 29] As already discussed above, I am also unable to agree with the Public Body that disclosing the existence of responsive records, if such exist, would serve to identify an informant. Confirming the existence of records responsive to portions of the Applicant's access request referring to an informant would confirm the existence of an informant; however, the evidence before me does not establish that the identity of such an informant would be revealed by doing so. It would appear that any information that would serve to reveal the identity of a putative informant could be redacted from records in which it appears by the application of section 20(1)(d) to any such information, if it exists.

Would confirming the existence of responsive records disclose the personal information of a third party?

[para 30] As discussed above, I find that if the Public Body were to confirm the existence of responsive records, then the Public Body would be possibly be confirming one or more of the following statements:

- A named member of a police department had a sexual relationship with an informant
- The police officer became the subject of a disciplinary investigation and an ASIRT investigation because of this relationship
- The police officer committed suicide.

[para 31] Section 1(n) of the FOIP Act defines personal information. This provision states:

1 In this Act.

(n) "personal information" means recorded information about an identifiable individual, including

- (i) the individual's name, home or business address or home or business telephone number,
- (ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
- (iii) the individual's age, sex, marital status or family status,
- (iv) an identifying number, symbol or other particular assigned to the individual,
- (v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
- (vi) information about the individual's health and health care history, including information about a physical or mental disability,
- (vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,
- (viii) anyone else's opinions about the individual, and
- (ix) the individual's personal views or opinions, except if they are about someone else [...]
- [para 32] In my view, confirming the existence of responsive records would confirm the facts alleged by the Applicant. Confirming the existence of any such alleged facts would reveal personal information of the police member who is the subject of the Applicant's allegations. I make this finding because confirming the existence of responsive records would confirm the statements I have set out above. Confirming these statements would constitute personal information about the police member who is the subject of the Applicant's allegations as an identifiable individual.
- [para 33] As discussed above, section 12(2)(b) may be applied only when it would be an unreasonable invasion of a third party's privacy to disclose the existence of personal information. It is therefore necessary to consider section 17 of the FOIP Act, which sets out the circumstances when it is, and when it is not, an invasion of a third party's personal privacy to disclose a third party's personal information.

Would it be an unreasonable invasion of a third party's personal privacy to disclose the existence of responsive records, if such exist?

## [para 34] Section 17 of the FOIP Act states, in part:

- 17(1) The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.
  - (2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if

*[...1* 

- (i) the personal information is about an individual who has been dead for 25 years or more, [...]
- (4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if
  - (a) the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation,
  - (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,

[...]

(d) the personal information relates to employment or educational history,

[...]

- (g) the personal information consists of the third party's name when
  - (i) it appears with other personal information about the third party, or
  - (ii) the disclosure of the name itself would reveal personal information about the third party,

or

- (h) the personal information indicates the third party's racial or ethnic origin or religious or political beliefs or associations.
- (5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether
  - (a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny,
  - (b) the disclosure is likely to promote public health and safety or the protection of the environment,
  - (c) the personal information is relevant to a fair determination of the applicant's rights,

- (d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,
- (e) the third party will be exposed unfairly to financial or other harm,
- (f) the personal information has been supplied in confidence,
- (g) the personal information is likely to be inaccurate or unreliable,
- (h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant, and
- (i) the personal information was originally provided by the applicant.

[para 35] Section 17 does not say that a public body is *never* allowed to disclose third party personal information. It is only when the disclosure of personal information would be an unreasonable invasion of a third party's personal privacy that a public body must refuse to disclose the information to an applicant under section 17(1). Section 17(2) establishes that disclosing certain kinds of personal information is not an unreasonable invasion of personal privacy.

[para 36] When the specific types of personal information set out in section 17(4) are involved, disclosure is presumed to be an unreasonable invasion of a third party's personal privacy. To determine whether disclosure of personal information would be an unreasonable invasion of the personal privacy of a third party, a public body must consider and weigh all relevant circumstances under section 17(5), (unless section 17(3), which is restricted in its application, applies). Section 17(5) is not an exhaustive list and any other relevant circumstances must be considered.

[para 37] In *University of Alberta v. Pylypiuk*, 2002 ABQB 22, the Court commented on the interpretation of what is now section 17. The Court said:

In interpreting how these sections work together, the Commissioner noted that s. 16(4) lists a set of circumstances where disclosure of a third party's personal information is presumed to be an unreasonable invasion of a third party's personal privacy. Then, according to the Commissioner, the relevant circumstances listed in s. 16(5) and any other relevant factors, are factors that must be weighed either in favour of or against disclosure of personal information once it has been determined that the information comes within s. 16(1) and (4). In my opinion, that is a reasonable and correct interpretation of those provisions in s. 16. Once it is determined that the criteria in s. 16(4) is [sic] met, the presumption is that disclosure will be an unreasonable invasion of personal privacy, subject to the other factors to be considered in s. 16(5). The factors in s. 16(5) must then be weighed against the presumption in s. 16(4). [my emphasis]

Section 17(1) requires a public body to withhold information only once the head has weighed all relevant interests in disclosing and withholding the information under section 17(5) and, having engaged in this process, the head concludes that it would be an unreasonable invasion of the personal privacy of a third party to disclose his or her personal information.

[para 38] In a case where section 12(2)(b) is applied, the question is whether, once all relevant interests weighing for or against disclosure are considered, disclosing the existence of the records would be an unreasonable invasion of personal privacy.

## [para 39] The Applicant argues:

Section 17(5) sets out a list of criteria to be sued to rebut the presumption under section 17(1) or 17(4) that disclosure of a third party's personal information would be an unreasonable invasion of personal privacy. Section 17(5) is not an exhaustive list of criteria to be considered when determining whether or not the presumption under s. 17(1) or s. 17(4) has been rebutted; other relevant factors may be considered.

[...]

In this case, several relevant factors weigh in favor of disclosing the existence of the record. The application of the relevant criteria is outlined below.

[...]

The Applicant submits that in this case, the relevant elements have been established and s. 17)(5)(a) applies. The allegation that a police officer was in a sexual relationship with a civilian informant has serious implications for the criminal justice system. A court has to determine if information provided by a confidential informant in an ITO is reliable before it will grant a search warrant or a wiretap authorization. If a court knew that the informant was in a sexual relationship with a police detective, a court might not accept the police officer's evidence based on the information an informant provided because the officer would be biased. The officer would be concerned about maintaining the relationship and could be motivated not to disclose information reflecting badly on the informant. If the information was being paid, the concerns are heightened. The officer would be motivated to pay her which requires she be reliable and provide reliable information.

Justice MacInnes of the Manitoba Court of Queen's Bench wrote the following about the justice system's concerns with informants:

While it is likely the case that most judges believe that informants do not provide information to the police for altruistic reasons, still, evidence as to the payment or favors provided, if known, are relevant in weighing the credibility of the informant and the reliability of his information. To suggest otherwise flies in the face of the reality of the justice system's ongoing, but particularly recent ongoing, and high-profile concerns about the reliability of the testimony of paid informants. *R. v. Brar* 2008 MBQB 1 at para 34

Therefore, people may have been improperly searched, prosecuted, and convicted based on what [the police officer] said his informant told him.

In addition, the sexual relationship must be disclosed by the Crown and, in turn, to the Defence as it is relevant in regard to the informant's reliability and the credibility of [the police officer]. If this disclosure was not made and a person was convicted, then a court might overturn a conviction. The Applicant is concerned that persons may have been convicted based on information the informant provided and the Crown did not disclose this information to such persons before or after the conviction. The Crown's disclosure obligation does not end after conviction.

[...]

The CTLA has been pressing the Public Prosecution Service for information about this [...]

Although only the Applicant has requested public scrutiny on this issue, the Applicant submits that because people could have been falsely convicted based on this information, this matter is such that it would be of concern to the broader community if they were to gain knowledge. The public would be concerned if the Crown did not take steps to overturn a conviction or to provide this information to a convicted person as they are required by law.

The public has granted police officers powers not available to ordinary citizens, so they can investigate crime. The public would want to be aware of the extent of police misconducts in general because this can influence the extent of power they give police officers and the oversight of the police. If such police misconducts are hidden under the veil of privacy, then the public would not be able to properly balance the powers they give police officers and its oversight, with the chance that this power might be abused. In this case, the public would want to know whether the informant had a sexual relationship with [the police officer] because of his position as a police officer and what the police did about it when it was discovered. For example, did the police immediately alert the Crown and conduct a review of all of [the police officer's] files?

[para 40] The Applicant also drew my attention to Orders 2000-012 and F2011-001, which hold that it is not always an unreasonable invasion of personal privacy to disclose the personal information of a deceased individual who has not been deceased for twenty-five years or more within the terms of section 17(2)(i). Order F2011-001 also holds that the privacy interests of a deceased person diminish over time. The longer an individual has been deceased, the lesser the privacy interest.

## [para 41] The Public Body argues:

If the fact scenario alleged by the Applicant were true, which the Public Body neither confirms nor denies, the Public Body submits that the disclosure would be an unreasonable invasion of third parties' personal privacy for the following reason, as outlined further below:

- Nothing in section 17(2) of the Act states that such disclosure would not be an unreasonable invasion of personal privacy.
- There is certainty against disclosure under sections 17(4), (b), (d), (g), and (h) of the Act.
- There are relevant circumstances against disclosure under section 17(5) of the Act.
- There are no relevant circumstances for disclosure under section 17(5) of the Act.

As per section 17(4)(b), if the fact scenario alleged by the Applicant were true, [...] the Public Body maintains that the disclosure of third party personal information identifiable as part of a law enforcement record, would be an unreasonable invasion of personal privacy.

Per section 17(4)(d), if the fact scenario alleged by the Applicant were true, [...], the Public Body maintains that the disclosure of third party personal information relating to employment history, would be an unreasonable invasion of personal privacy.

In addition, as per section 17(4)(g), if the fact scenario alleged by the Applicant were true, [...], the Public Body maintains that the identification of any third parties by name along with any

other potential personal information would be an unreasonable invasion of their personal privacy.

Further, as per section 17(4)(h), if the fact scenario alleged by the applicant were true, [...], the Public Body maintains that the disclosure of third party personal information relating to their associations, would be an unreasonable invasion of their personal privacy.

The Public Body reviewed all circumstances under section 17(5) of the Act and maintains that, if the fact scenario alleged by the Applicant were true, [...], the circumstances weigh in favour of non-disclosure of the personal information.

In regard to section 17(5)(a) of the Act, the Public Body submits that the fact scenario alleged by the Applicant, [...], does not involve any activity of the Public Body that should be subject to public scrutiny. The fact scenario is speculation with respect to criminal activity that the Applicant believes occurred. To the extent that there is any activity that should be subject to public scrutiny, it is the alleged criminal activity. The Public Body submits that disclosure under the Act is not the appropriate manner in which alleged criminal activity should be subject to public scrutiny; the appropriate forum for such scrutiny is in court.

The Public Body submits that section 17(5)(a) weighs against disclosure.

As per section 17(5)(e), if the fact scenario alleged by the Applicant were true, [...] the Public Body maintains that third parties would be harmed with respect to their personal safety if the existence or non-existence of the records was disclosed as per the Applicant's request for "a copy of the final report of ASIRT... and information provided by the informant "pertaining to allegations "that [police officer] was in a sexual relationship with an informant..."

Further as per section 17(5)(f), if the fact scenario alleged by the Applicant were true, [...], the Public Body maintains that third parties would have provided the information in explicit confidence to ASIRT investigators with the understanding that such information would remain private and confidential.

Section 17(4)

[para 42] As discussed above, the information that would be disclosed by confirming the existence of the records, if such exist, would be the following:

- A named member of a police department had a sexual relationship with an informant.
- The police officer became the subject of a disciplinary investigation and an ASIRT investigation because of this relationship.
- The police officer committed suicide.

[para 43] I find that this information falls within section 17(4)(g) of the FOIP Act (reproduced above) as it consists of the police member's name in the context of other information about him. As a result, a presumption arises that it would be an unreasonable invasion of a third party's personal privacy to disclose the existence of responsive records. It is therefore necessary to weigh relevant considerations under section 17(5) in order to determine whether the presumption is rebutted.

*Section* 17(5)

[para 44] The Applicant argues that it would not be an invasion of a third party's personal privacy to confirm or deny the existence of responsive records, or to provide any such responsive records to it because a public interest would be served by disclosing responsive information and because the third party's privacy interests are diminished because the third party is deceased.

[para 45] The Public Body argues that it would be an unreasonable invasion of the third party's personal privacy to confirm or deny the existence of responsive records, or to provide any such records to the Applicant. The Public Body argues that section both sections 17(5)(a) and (f) of the FOIP Act, (reproduced above) weigh against disclosing such information to the Applicant.

*Is section* 17(5)(a) *of the FOIP Act a relevant factor?* 

[para 46] Cited above, section 17(5)(a) states:

17(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny,

[para 47] In Order F2010-010, the Adjudicator considered the application of section 17(5)(a) in a case where the Edmonton Police Service had elected neither to confirm nor deny the existence of records relating to the investigation, arrest, and resignation of a police officer. She said:

In my view, due to the interplay of section 12(2) of the Act and section 17 of the Act, and the facts and arguments before me, I am required to consider if section 17(5)(a) of the Act is applicable. If it is, I must then decide if the need for public scrutiny outweighs the other relevant factors in section 17(5) of the Act, and overrides the presumptions that disclosure of the existence of the information would be an unreasonable invasion of a third party's personal privacy.

The Applicant argues that the public interest in this matter – dealing with how the Public Body investigates and disciplines its own members – is paramount over any claim to third party personal privacy. The Public Body argues that any public interest in this matter is not sufficient to override the privacy interests applicable in this inquiry. It states:

An expressed "concern" regarding the laying or not laying of criminal charges in a particular matter that the Applicant alleges is not sufficient to show a public interest that overcomes a privacy interest in any responsive records. The concern does not rise to the level of public interest required for section 17(5)(a) to overcome the application of all of the other relevant elements in section 17(5).

As noted above, the Applicant has said that the EPS officer in question had been investigated, arrested, and resigned or retired as the result of these incidents. The Applicant has also presented some evidence which may, possibly, be taken as suggesting that these things happened. Leaving aside for the moment whether the evidence presented by the Applicant is sufficient to establish that these things happened in fact, I will consider the position if, hypothetically, such events did happen and there are records relating to them, is public scrutiny called for?

In cases involving improper or illegal behaviour by police officers or allegations thereof, public scrutiny may be a relevant factor both because the public needs to know how the Public Body deals with the behaviour or alleged behaviour, as well as, in some cases, because the public needs to know which individual police officers have engaged in wrongful behaviour.

The decisions of this office have held that, for disciplinary matters, scrutiny of the disciplinary process can be achieved without naming individual officers. As well, information relating to the officers themselves is to be disclosed where they have been found to have engaged in certain kinds of wrongful conduct. In the CPS decision mentioned above, the court reviewed a decision of this office and decided that the public membership of the Law Enforcement Review Board ("LERB"), the Calgary Police Commission, and potential scrutiny by the Minister of Justice in relation to any provincial or federal offences, provides adequate scrutiny, and that limited individual officer's information is to be disclosed only in circumstances where the member's actions may constitute a federal or provincial offence.

[para 48] The Adjudicator in that case asked herself the question, "If such events did happen and there are records relating to them, is public scrutiny called for?" I agree that this is the question that must be asked in this case.

[para 49] As discussed above, the events the Applicant alleges are the following:

- A member of a police department had a sexual relationship with an informant.
- The member became the subject of a disciplinary investigation and an ASIRT investigation because of this relationship.
- The member committed suicide.

[para 50] The Applicant argues he requires not only confirmation of the existence of the records, but the records themselves, because search warrants could have been authorized based on statements made by the informant. He argues that any such warrants had the potential to have been issued on the basis of biased information, given the informant's alleged relationship with the police officer. He reasons that people could possibly have been convicted on the basis of evidence obtained from an improperly issued search warrant and that there is, as a result, a need for public scrutiny of the activities of the Public Body or police services.

[para 51] The theory that warrants may have been issued on the basis of inaccurate information given that there was a relationship between the officer (swearing whatever information it would be necessary to swear) and an informant (giving the information to which the officer would swear and which would form the foundation for a warrant) is too speculative to form the basis of a suspicion that there may have been a miscarriage of justice in issuing such warrants.

[para 52] Moreover, there is nothing before me to suggest that the actions the Applicant attributes to the police member are part of a widespread problem among police members in Alberta, as opposed to an isolated incident. It has not been established that the processes in place in the judicial system to ensure that search warrants are not issued without reasonable and probable grounds for doing so are inadequate, or would have failed in the scenario described by the Applicant. As a result, it has not been established that public scrutiny of this case is necessary to reveal a systemic problem or to prevent or rectify a miscarriage of justice. In other words, it has been established for this inquiry that the procedural safeguards in place in the justice system to ensure that searches are not conducted without reasonable and probable grounds failed, or would fail, in the hypothetical circumstances presented by the Applicant.

[para 53] There is also no evidence before me to establish that the measures that the Applicant states were taken to address the alleged misconduct of the police member – a disciplinary suspension and an ASIRT investigation under section 46.1 of the *Police Act* – were inadequate to reduce the likelihood of incidents similar to that alleged by the Applicant taking place in Alberta.

[para 54] In its rebuttal submissions, the Applicant took issue with the following statement made by the Public Body in its initial submissions:

To the extent that there is any activity that should be subject to public scrutiny, it is the alleged criminal activity. The Public Body submits that disclosure under the Act is not the appropriate manner in which alleged criminal activity should be subject to public scrutiny; the appropriate forum for any such scrutiny is in court.

## [para 55] In its rebuttal submissions, the Public Body countered:

While there may not be criminal charges in regard to the allegations made against the named [...] member, it is reasonable to conclude there are other more appropriate legal avenues to identify if the allegations are in fact real that would better protect the personal information of the alleged named police service member, the alleged "informant" and any other unknown individuals whose personal information could be disclosed by confirming or denying the existence of responsive records.

[para 56] It is unclear to me what the criminal activity would be on the facts alleged in the Applicant's access request, or how it would be possible for this criminal activity to be addressed by the courts, given the Applicant's allegation that the police member is deceased. It is also unclear what the "other more appropriate legal avenues", to which the Public Body refers, may be, or whether it would be reasonable to conclude that these legal avenues are more appropriate for investigating allegations.

[para 57] Section 46.1of the *Police Act*, under which ASIRT may be asked to investigate, states, in part:

46.1(1) The chief of police shall as soon as practicable notify the commission and the Minister where

- (a) an incident occurs involving serious injury to or the death of any person that may have resulted from the actions of a police officer, or
- (b) a complaint is made alleging that
  - (i) serious injury to or the death of any person may have resulted from the actions of a police officer, or
  - (ii) there is any matter of a serious or sensitive nature related to the actions of a police officer.
- (2) The Minister, when notified under subsection (1) of an incident or complaint or on the Minister's own initiative where the Minister becomes aware of an incident or complaint described in subsection (1), may do any one or more of the following:

[...]

(d) in accordance with section 46.2, direct the head of an integrated investigative unit to conduct an investigation into the incident or complaint, which may include taking over an ongoing investigation at any stage.

[...]

- [para 58] Section 46.1 of the *Police Act* contains a mechanism by which police members are held to account for their actions in matters of a sensitive or serious nature. The actions the Applicant attributes to the police member would possibly be an example of actions giving rise to a matter of a sensitive or serious nature.
- [para 59] If the police member was suspended and ASIRT conducted an investigation, then these are processes by which the Applicant's allegations regarding the police member's alleged affair with an informant would be investigated. So while it is unclear to me what the Public Body means by "other legal avenues" in its submissions, it is clear that the suspension and the ASIRT investigation to which the Applicant refers would be processes by which the allegations of the kind made by the Applicant would have been investigated and scrutinized, if such an investigation were conducted.
- [para 60] As discussed above, I am unable to find that the allegations made by the Applicant, if true, would reflect anything more than an isolated incident. Moreover, I am unable to find that the procedural safeguards in place in the justice system to ensure that warrants are not issued without sufficient grounds to do so would have failed in the circumstances projected by the Applicant, even had it been established that the alleged informant provided information that formed the basis of a search warrant.
- [para 61] Assuming the ASIRT investigation the Applicant alleges took place did take place, this process would have subjected the actions the Applicant attributes to the

police member to an appropriate degree of scrutiny. The Applicant has not established that this process would have been flawed in any way, or would have involved an inadequate investigation. It is therefore unclear why further scrutiny of the actions the Applicant alleges would be necessary.

[para 62] For these reasons, I find that section 17(5)(a) is not engaged. However, the fact that I find that section 17(5)(a) does not apply does not mean that section 17(5)(a) weighs *against* disclosure, as the Public Body appears to suggest in its submissions, where it states: "The Public Body submits that section 17(5)(a) weighs against disclosure." Rather, as section 17(5)(a) does not apply, it is an irrelevant consideration, neither weighing for nor against disclosure.

*Is section* 17(5)(f) *a relevant factor?* 

[para 63] Section 17(5)(f) applies when a third party's personal information has been supplied by a third party in confidence. When it applies, section 17(5)(f) weighs against disclosure.

[para 64] It is unclear to me how section 17(5)(f) could be said to apply in this case. The Public Body "maintains that third parties would have provided the information in explicit confidence to ASIRT investigators with the understanding that such information would remain private and confidential". However, the issue before me in relation to the application of section 12(2)(b) is whether it would be an unreasonable invasion of a third party's personal privacy to disclose the existence of personal information responsive to the Applicant's access request. As discussed above, the information that would be revealed by disclosure of the existence of responsive records is the following: that a police member had an affair with an informant; that the police member was suspended, that the police member committed suicide, and that ASIRT conducted an investigation. None of this information could be said to have been "supplied" or "given" by the police member to anyone, in confidence or otherwise. Rather, if it existed it would be information "about" him as an identifiable individual.

[para 65] In addition, section 46.1 of the *Police Act*, cited above, under which ASIRT derives its authority to investigate serious incidents, imposes a duty on ASIRT to provide a report to the Minister of Justice and Solicitor General, to refer matters to the Minister of Justice and Solicitor General, and to advise the applicable police commission and chief of police of its findings in particular circumstances. Given these reporting and referral obligations, I am unable to agree with the Public Body that information supplied to ASIRT is necessarily supplied in confidence.

[para 66] I find that section 17(5)(f) is an irrelevant consideration in this inquiry and weighs neither for nor against disclosure.

Does the fact that the third party whose information is the subject of the access request is deceased weigh in favor of disclosing the existence of responsive records?

[para 67] In Order F2012-24, the Director of Adjudication considered the extent to which death of a third party is relevant to a determination under section 17(5) of the FOIP Act. She said:

Before leaving this factor I will comment on the significance to the issue in this case of section 17(2)(i), since the Public Body has cited this provision with reference to the application of section 17 (at paras 3 and 23). Section 17(2)(i), provides that it is not an unreasonable invasion of privacy to disclose the personal information of someone who has been dead for 25 years or more. It is not the case, however, that the expectation of privacy of an individual does not change once the individual has died.

In Order F2011-001 the Adjudicator said:

The Public Body notes that the Complainant's mother died in 1996. As she has not been dead for twenty-five years, the Public Body correctly points out that section 17(2)(i) does not apply to personal information about her. If section 17(2)(i) applied, it would not be an unreasonable invasion of personal privacy to disclose the personal information and it would be unnecessary to weigh competing interests under section 17(5). However, the converse is not true: it does not follow from the fact that section 17(2)(i) does not apply that disclosure is an unreasonable invasion of personal privacy.

In other words, section 17(2)(i) does not operate 'in reverse', and the fact that an individual has not been dead for twenty-five years does not mean that it would necessarily be an unreasonable invasion of the individual's personal privacy to disclose information about the individual.

The Adjudicator also found in Order F2011-001 that the privacy interests of deceased individuals diminish over time and that this may be a consideration under section 17(5). She said:

The former Information and Privacy Commissioner of Ontario considered that the fact that an individual is deceased is a factor to be weighed when deciding whether it would be an unreasonable or unjustifiable invasion of personal privacy to disclose personal information. In his view, that an individual is deceased, while only one of several factors he considered in that case, was nevertheless a factor weighing in favor of disclosure. I agree with this analysis and share the view that individual privacy interests diminish after death. If privacy interests do not diminish following death and over time, it would be entirely arbitrary for the legislature to determine that privacy rights end after twenty-five years when they do not after twenty-four years and eleven months, for example.

I agree that the privacy interests of a deceased person may diminish over time. In the case before me, the Applicants' daughter has been dead for over five years. Disclosing her personal information now would not necessarily be an invasion of her personal privacy to the same extent that it would have been in her lifetime. That is another consideration that is relevant to the application of section 17(5) in this case.

[para 68] As the Applicant points out, previous orders of this office have stated that the privacy interests of deceased persons diminish over time. However, that does not mean that there are no privacy interests attached to their personal information, or that a presumption created by a provision of section 17(4) is rebutted solely because the third party is deceased.

[para 69] In Order F2012-24, cited above, the Director of Adjudication found that a deceased third party's privacy interests were diminished by the fact that the third party had been deceased for five years; however, she also found that compassionate considerations weighed very strongly in favor of disclosure.

[para 70] In Order F2011-001, I found that the privacy interests of an applicant's deceased mother were diminished fifteen years after her death. I also found that the fact that the mother's personal information was also information about the applicant's own family and medical history weighed in favor of disclosure.

[para 71] Orders F2012-24 and F2011-001 are distinguishable on the basis that factors weighing in favor of disclosure were found to be relevant to the decision to be made under section 17(5). In the present case, I am unable to identify any public interest in disclosing the existence of the records, or the kinds of personal information that the Applicant argues responsive records would contain. If the allegations of the Applicant are true, the privacy interests the deceased officer had in his personal information may be diminished to a certain extent, by virtue of being deceased. However, that does not mean that all privacy interests are extinguished. In the absence of a factor weighing in favor of disclosure, I find that the presumption created by section 17(4)(g) has not been rebutted.

#### Conclusion

[para 72] As confirming the existence of responsive records, if any exist, would serve to reveal personal information subject to the presumption created by section 17(4)(g), and as there is no basis on which this presumption could be rebutted, I confirm the decision of the Public Body not to confirm or deny the existence of responsive records.

#### IV. ORDER

[para 73] I make this Order under section 72 of the Act.

[para 74] I find that the Public Body properly refused to confirm or deny the existence of a record under section 12(2)(b) of the Act, and I confirm its decision to do so.

Teresa Cunningham	
Adjudicator	