Protecting privacy. Promoting transparency.

Order F16-28

INDEPENDENT INVESTIGATIONS OFFICE

Elizabeth Barker
Senior Adjudicator

June 8, 2016

CanLII Cite: 2016 BCIPC 30
Quicklaw Cite: [2016] B.C.I.P.C.D. No. 30

Summary: The applicant requested records relating to his employment with the IIO. The IIO withheld records and information under s. 3(1)(c) (outside scope of Act), s. 13 (policy advice and recommendations), s. 14 (solicitor client privilege), s. 15 (harm to law enforcement), s. 16(1)(b) (harm to intergovernmental relations), and s. 22 (harm to personal privacy) of FIPPA. The adjudicator confirmed the IIO's decision regarding ss. 3(1)(c), 13, 14, 16(1)(b) and 22. The adjudicator determined that the IIO was not authorized to refuse the applicant access to information under s. 15 and required it give the applicant access to that information (subject only to information that it was authorized to refuse to disclose under the other exceptions).

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, ss. 3(1)(c), 13, 14, 15(1)(a), 15(1)(c), 15(1)(d), 16(1)(b), 22 and Schedule 1 definitions of "officer of the Legislature" and "law enforcement".

Authorities Considered: B.C.: Order 36-1995, [1995] B.C.I.P.C.D. No. 8; Order 170-1997, 1997 CanLII 1485 (BCIPC); Order 331-1999, 1999 CanLII 4253 (BCIPC); Order 00-01, 2000 CanLII 9670 (BCIPC); Order 00-18, 2000 CanLII 7416 (BCIPC); Order 00-52, 2000 CanLII 14417 (BCIPC); Order 01-07, 2001 CanLII 21561 (BC IPC); Order 01-15, 2001 CanLII 21569 (BC IPC); Order 01-43, 2001 CanLII 21597 (BCIPC); Order 01-53, 2001 CanLII 21607 (BC IPC); Order 02-19, 2002 CanLII 42444 (BC IPC); Order 02-38, 2002 CanLII 42472 (BCIPC); Order 03-14, 2003 CanLII 49183 (BC IPC); Order 03-35, 2003 CanLII 49214 (BCIPC); Order F07-17, 2007 CanLII 35478 (BC IPC); Order F08-02, 2008 CanLII 1645 (BC IPC); Order F08-08, 2008 CanLII 21700 (BCIPC); Order F10-15, 2010 BCIPC 24 (CanLII); Order F11-06, 2011 BCIPC 7 (CanLII); Order F13-10, 2013 BCIPC 11 (CanLII); Order F13-23, 2013 BCIPC 30 (CanLII); Order F14-10, 2014

BCIPC 12 (CanLII); Order F14-12, 2014 BCIPC 15; Order F14-41, 2014 BCIPC 44; Order F15-26, 2015 BCIPC 23 (CanLII).

Cases Considered: *Canada v. Solosky*, 1979 CanLII 9 (SCC); *John Doe v. Ontario (Finance*), 2014 SCC 36; *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner), 2014 SCC 31; College of Physicians of B.C. v. British Columbia (Information and Privacy Commissioner),* 2002 BCCA 665; *Maximum Ventures Inc. v. De Graaf*, 2007 BCCA 510; *Gower v. Tolko Manitoba Inc*., 2001 MBCA 11; *R. v. B.,* 1995 CanLII 2007 (BCSC); *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner), 2012 BCSC 875; S & K Processors Ltd. v. Campbell Ave. Herring Producers Ltd*., 1983 CanLII 407 (BCSC); *Le Soleil Hotel & Suites Ltd. v. Le Soleil Management Inc., 2007 BCSC 1420; Maximum Ventures Inc. v. de Graaf***,** 2007 BCSC 1215.

INTRODUCTION

[1] This inquiry is about an applicant's request for records relating to his former employment with the Independent Investigations Office ("IIO"). The IIO disclosed some records to the applicant after severing information from them under s. 13 (policy advice and recommendations), s. 14 (solicitor client privilege), s. 15 (harm to law enforcement), s.16 (harm to intergovernmental relations), s. 17 (harm to financial or economic interests of a public body) and s. 22 (harm to personal privacy) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"). In addition the IIO severed some information from the records on the basis that it was not responsive to the access request. It also withheld some records on the basis that s. 3(1)(c) applied and they are outside the scope of FIPPA.

[2] The applicant requested a review of the IIO's decision by the Office of the Information and Privacy Commissioner ("OIPC"). Mediation did not resolve the issues and the applicant requested that they proceed to a written inquiry.

[3] The Notice of Inquiry states that s. 17 is at issue in this inquiry. During the inquiry, however, the IIO clarified that it is no longer withholding information under s. 17 and would rely on other exceptions. The applicant said that he is only interested in gaining access to one of those two excerpts that had originally been withheld under s. 17.[1] The IIO is now withholding it under ss. 13 and 14.

[4] Also, during the course of the inquiry, the IIO discovered an additional 40 pages of records, which it determined were responsive to the applicant's access request.[2] The IIO disclosed them to the applicant after redacting information under ss. 13, 15, 16, 22 and on the basis that it is "not responsive".[3] The IIO said

[1] Large set: p. 374.
[2] IIO's initial submissions, para. 3.06 and reply submissions, para. 1.
[3] It is unclear when exactly these 40 pages were disclosed to the applicant.

that these 40 pages were not in dispute. The applicant said he wanted access to this information and disputed the IIO's decision to withhold it. Ultimately, I decided that that those 40 pages and the IIO's decision to refuse the applicant access to information in them were also at issue in the inquiry.[4] In this decision, I will refer to these 40 pages as the "small set" of records and the balance of the records (472 pages) as the "large set" of records.

[5] The Investigator's Fact Report and the Notice of Inquiry did not include the issue of the IIO withholding information as "not responsive".[5] Therefore, I wrote to the parties seeking submissions. Ultimately, the IIO reconsidered its decision to withhold information as "not responsive" and it applied ss. 13, 14, 15, 16 and 22 instead.[6] The IIO also applied s. 21 (disclosure harmful to business interest of a third party) to some of that information.[7] The applicant said that he does not want access to the information being withheld under s. 21, so I will not consider the application of s. 21 to the records.

[6] Both parties provided an additional submission regarding the IIO's application of ss. 13, 14, 15, 16 and 22 to the small set of records and to the information that the IIO had previously withheld as being "not responsive.[8]

ISSUES

[7] The issues to be decided in this inquiry are as follows:

1. Do any of the records fall outside the scope of FIPPA, pursuant to s. 3(1)(c) of FIPPA?

2. Is the IIO authorized to refuse to disclose the information at issue under ss. 13, 14, 15 and/or 16 of FIPPA?

3. Is the IIO required to refuse to disclose the information at issue under s. 22 of FIPPA?

[8] Section 57 of FIPPA states the burden of proof at inquiry. The IIO has the burden of proving that the applicant has no right of access to the information it is refusing to disclose under ss. 13, 14, 15 and 16. However, the applicant must prove that disclosure of any personal information in the requested records would not be an unreasonable invasion of third party personal privacy under s. 22. Although s. 57 is silent regarding the burden in cases involving s. 3(1), previous

[4] My January 13 and 19, 2016 letters. The IIO also reconsidered its decision to withhold information from these 40 pages as "not responsive" and applied FIPPA exceptions instead.
[5] IIO initial submissions, para. 4.05.
[6] On November 30, 2015.
[7] Small set: p. 3.
[8] The IIO's submission is dated February 10, 2016. The applicant's submission dated February 23, 2016.

orders have established that the public body bears the burden of proving that the records are excluded from the scope of FIPPA.[9]

DISCUSSION

[9] **Background -** The IIO is a civilian led office, which investigates incidents of serious harm and death involving police officers in BC. The IIO was instituted under the *Police Act*[10] and is directed by a Chief Civilian Director ("Director"). Although the IIO is established within the Ministry of Justice, it is a public body in its own right pursuant to Schedule 2 of FIPPA.

[10] In January 2014, the IIO learned that an offer of employment letter had inadvertently been saved on the IIO's shared computer drive and had been accessed by several IIO investigators. For clarity, I will refer to this incident from this point forward as the "privacy concern".

[11] The Director asked the IIO's Director of Legal Services ("IIO Lawyer") to investigate the privacy concern. Approximately three weeks later, the Director asked the Office of the Police Complaints Commissioner ("OPCC")[11] to also investigate and to identify any IIO investigator who may have lied or participated in a breach of trust by covering up misconduct related to the privacy concern.[12]

[12] About two months after the discovery of the privacy concern, the IIO terminated the applicant's employment.

[13] **Information in Dispute -** As previously mentioned there are two sets of records in this inquiry: the "large set", which contains 472 pages and the "small set" with 40 pages. Specifically, the records are letters, emails, reports, hand written notes, copies of electronic calendars, employment related forms (e.g., benefits, emergency contacts, oaths), résumés, grids used to score job applicants, photos and written logs of investigative materials gathered from the applicant's workstation after his employment ended.

[14] Both parties say that the OPCC has disclosed some records related to its investigation to the applicant. However, their submissions do not specify which records or information the applicant received from the OPCC. Therefore, I have taken the approach that the applicant is still seeking access to all of the information being withheld by the IIO, including the records that clearly originated with the OPCC.

---

[9] For example: Order 170-1997, 1997 CanLII 1485 (BCIPC); Order 03-14, 2003 CanLII 49183 (BC IPC); Order F13-23, 2013 BCIPC 30 (CanLII).

[10] *[RSBC 1996] c. 367, Part 7.1.*

[11] The OPCC is established under the *Police Act*. It provides civilian oversight of complaints involving municipal police in BC.

[12] All of this information has previously been provided to the applicant. See large set: p. 47.

Scope of FIPPA (s. 3(1)(c))

[15] The IIO is relying on s. 3(1)(c) to withhold several emails[13] between the IIO and the Merit Commissioner regarding an audit of two IIO job competitions. Section 3(1)(c) states:

> 3(1) This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:
> ...
> (c) subject to subsection (3), a record that is created by or for, or is in the custody or control of, an officer of the Legislature and that relates to the exercise of that officer's functions under an Act; [Note: s. 3(3) is not relevant in this case].

[16] Previous OIPC orders have said that in order for s. 3(1)(c) to apply, the following criteria must be met:

1. An "officer of the Legislature" is involved.
2. The record must either:
    a. have been created *by* or *for* the officer of the Legislature; or
    b. be in the *custody* or *control* of the officer of the Legislature.
3. The record must relate to the exercise of the officer's functions under an Act.[14]

[17] The IIO submits that the emails were created for the Merit Commissioner and relate to Merit Commissioner's responsibilities as an officer of the Legislature - specifically, to monitor the application of the merit principle by auditing appointments under s. 5.1 of the *Public Service Act*.[15] The IIO says that the records withheld under s. 3(1)(c) contain communications between the IIO and the Merit Commissioner's staff regarding an audit of two IIO job competitions. The applicant makes no submissions regarding s. 3(1)(c).

[18] The Merit Commissioner is an officer of the Legislature under s. 3(1)(c) as the definition of "officer of the Legislature" in Schedule 1 of FIPPA specifically includes the Merit Commissioner appointed under the *Public Service Act*.

[19] The Merit Commissioner's functions are described, in part, under s. 5.1 of the *Public Service Act*, which says:

---

[13] Large set: pp. 192-199 and 201.
[14] Order 01-43, 2001 CanLII 21597 (BCIPC), para. 14; Order F14-12, 2014 BCIPC 15, para. 8.
[15] [RSBC 1996] c. 385.

> 5.1 (1) The merit commissioner is responsible for monitoring the application of the merit principle under this Act by
>
> (a) conducting random audits of appointments to and from within the public service to assess whether
>
> (i) the recruitment and selection processes were properly applied to result in appointments based on merit, and
>
> (ii) the individuals when appointed possessed the required qualifications for the positions to which they were appointed, and
>
> (b) reporting the audit results to the deputy ministers or other persons having overall responsibility for the ministries, boards, commissions, agencies or organizations, as the case may be, in which the appointments were made.

[20] The emails are the IIO's communications with a member of the Merit Commissioner's staff who was conducting an audit of an IIO job competition. It is obvious that these records were created by or for the Merit Commissioner and they clearly relate to the exercise of the Merit Commissioner's functions under s. 5.1 of the *Public Service Act*. I find that s. 3(1)(c) applies to the emails, so they are outside the scope of FIPPA.

Policy Advice or Recommendations (s. 13)

[21] The IIO is withholding several excerpts from the records under s. 13. Section 13(1) states that the head of a public body may refuse to disclose to an applicant information that would reveal advice or recommendations developed by or for a public body or a minister.

[22] Section 13(1) has been the subject of many orders, which have consistently held that the purpose of s. 13(1) is to allow full and frank discussion of advice or recommendations on a proposed course of action by preventing the harm that would occur if the deliberative process of government decision and policy-making were subject to excessive scrutiny.[16] BC orders have found that s. 13(1) applies not only when disclosure of the information would directly reveal advice and recommendations, but also when it would allow accurate inferences about the advice or recommendations.[17]

[23] The process for determining whether s. 13(1) applies to information involves two stages.[18] The first is to determine whether the disclosure of the information would reveal advice or recommendations developed by or for the public body. If so, then it is necessary to consider whether the information falls

[16] For example, Order 01-15, 2001 CanLII 21569 (BC IPC). See also *John Doe v. Ontario (Finance*), 2014 SCC 36 at para. 45.
[17] Order 02-38, 2002 CanLII 42472 (BCIPC); Order F10-15, 2010 BCIPC 24 (CanLII).
[18] Order F07-17, 2007 CanLII 35478 (BC IPC), para 18.

within any of the categories listed in s. 13(2). If it does, the public body must not refuse to disclose the information under s. 13(1).

[24] The IIO submits that the information it is withholding under s. 13 was developed by the Public Service Agency and the Ministry of Justice for the purpose of providing advice and recommendations to the IIO regarding the discipline and termination of employees. It also says that the information does not fall within s. 13(2). The applicant's only submission regarding s. 13 is that the Director did not follow the advice he was given.

[25] In my view, all of the information withheld under s. 13 is advice and recommendations. It either directly reveals advice and recommendations about the matters under consideration, or it would clearly allow accurate inferences about advice and recommendations. In addition, the information does not fall into any of the categories listed in s. 13(2). Therefore, I find that the IIO is authorized to refuse to disclose all of the information it is withholding under s. 13(1).

Solicitor client privilege (s. 14)

[26] Section 14 states that the head of a public body may refuse to disclose information that is subject to solicitor client privilege. The law is well established that s.14 encompasses both legal professional privilege, which is often referred to as legal advice privilege, and litigation privilege.[19]

[27] The IIO submits that legal advice privilege applies to the information it is withholding under s. 14.[20] Specifically, it says that the information is about legal advice sought and received on a confidential basis from the IIO Lawyer and lawyers with the Ministry of Justice's Legal Services Branch ("LSB").

[28] The applicant submits that the IIO is claiming privilege over the records in order to hide a biased investigation and an abuse of authority. He does not, however, submit that privilege does not apply.

[29] For legal advice privilege to apply the following conditions must be satisfied:

1. there must be a communication, whether oral or written;
2. the communication must be confidential;

[19] *College of Physicians of B.C. v. British Columbia (Information and Privacy Commissioner),* 2002 BCCA 665 at para. 26.

[20] I will not consider the IIO's application of s. 14 to the information that I have already found may be withheld under s. 13(1).

3. the communication must be between a client (or agent) and a legal advisor; and
4. the communication must be directly related to the seeking, formulating, or giving of legal advice.

[30] Not every communication between client and solicitor is protected by solicitor client privilege, but if the four conditions above are satisfied, then privilege applies to the communications and the records relating to it.[21] The above criteria have consistently been applied in BC orders, and I will take the same approach here.[22]

[31] The IIO has applied s. 14 to withhold information that is unrelated to the privacy concern as well as to information that relates directly to the IIO Lawyer's investigation of the privacy concern. I will consider each separately below.

[32] It is apparent that s. 14 has been applied, for the most part, to records and excerpts of records that are unrelated to the privacy concern. They are written communications among IIO staff, the IIO's Lawyer and LSB lawyers.[23] There are also several pages of communications between the IIO Lawyer, the Director and other IIO staff.[24] All of these communications involve at least one lawyer. It is clear from the content and context of these records that they are communications made for the purpose of seeking and giving legal advice. The IIO submits that these communications were made with the expectation of confidentiality and the records have been treated as such by the IIO. Further, the Director deposes that the communications comprise legal advice the IIO sought and received on a confidential basis from its lawyers.[25] The signature block of some of the records contains a statement to the effect that the email is privileged and confidential and intended to be seen by the addressee only. Moreover, there is nothing to suggest that these communications were not kept confidential between the IIO and LSB lawyers. I am satisfied, therefore, that they were confidential communications between solicitor and client. In conclusion, I find that these communications, which are unrelated to the privacy concern, meet the criteria for legal advice privilege.

[33] The balance of the excerpts withheld under s. 14 reveal the IIO Lawyer's communications during his investigation of the privacy concern. The IIO submits that the IIO Lawyer's investigation and his communications with IIO employees took place for the purpose of giving legal advice to the IIO.

---

[21] *R. v. B.,* 1995 CanLII 2007 (BCSC) at para. 22. See also *Canada v. Solosky*, 1979 CanLII 9 (SCC) at p. 13.
[22] See: Order 01-53, 2001 CanLII 21607 (BC IPC) and Order F13-10, 2013 BCIPC 11 (CanLII).
[23] Large set: pp. 31-38 (duplicate at 276-283); 83 (duplicate at 298), 301-304, 308, 317-329, 334-347, 374-387, 390 and 397-400.
[24] Large set: pp. 140, 149-154, 156-162, 229, 431-36, 438 and 439.
[25] Director's affidavit #1, para. 32.

[34] The BC Court of Appeal in *College of Physicians of B.C. v. British Columbia (Information and Privacy Commissioner*)[26] [*College*] said the following about investigations conducted by lawyers:

> [32] …Legal advice privilege arises only where a solicitor is acting as a lawyer, that is, when giving legal advice to the client. Where a lawyer acts only as an investigator, there is no privilege protecting communications to or from her. If, however, the lawyer is conducting an investigation for the purposes of giving legal advice to her client, legal advice privilege will attach to the communications between the lawyer and her client (see Gower at paras. 36-42)…
>
> [39] …Lawyers must often undertake investigative work in order to give accurate legal advice. In this respect, investigation is integral to the lawyer's function.
>
> [40] The nature of investigative work undertaken by a lawyer was discussed in *Gower* (at para. 19):
>
> > ...legal advice is not confined to merely telling the client the state of the law. It includes advice as to what should be done in the relevant legal context. It must, as a necessity, include ascertaining or investigating the facts upon which the advice will be rendered. Courts have consistently recognized that investigation may be an important part of a lawyer's legal services to a client so long as they are connected to the provision of those legal services.

[35] In the present case, the records themselves as well as the Director's affidavit (which includes a copy of the IIO Lawyer's job description) provide information about the IIO Lawyer's role during his investigation of the privacy concern. In considering this information, I have kept in mind that *College* says, "… the key question to consider is whether the communication is made for the purpose of seeking or providing legal advice, opinion or analysis."[27]

[36] The Director says that when he learned of the privacy concern, he asked the IIO Lawyer to investigate. He also says:

> Responsibility for investigating privacy breaches is included in the job description for legal counsel at the IIO. I expected that [IIO Lawyer] would be acting within his capacity as legal counsel for the IIO when conducting investigations into privacy breaches… I expected [IIO Lawyer] would conduct an investigation and provide me with legal advice with respect to the breach. I also expected that part of [IIO Lawyer's] investigation would include interviewing witnesses in order to provide this advice.[28]

---

[26] *College*, supra note 19, at paras. 32, 39, 40. Reference to *Gower v. Tolko Manitoba Inc*., 2001 MBCA 11.
[27] *College*, supra note 19, at para. 31.
[28] Director's affidavit #1, para. 38-40.

[37] The IIO's Lawyer's job description states that the incumbent will serve as in-house legal counsel to the IIO and provide advice on criminal law, corporate and operational issues and supervise records management, information security and disclosure under FIPPA.

[38] Based on the content and context of the records in dispute, I am satisfied that the IIO Lawyer investigated the privacy concern in his capacity as the IIO's lawyer. I am also convinced that his communications with IIO staff regarding the privacy concern relate to formulating and providing legal advice regarding the legal implications of that matter. Although the records do not themselves contain explicit statements of legal advice or opinion, the Director deposes that the IIO Lawyer did, in fact, provide him with "legal advice as to what should be done in the legal context identified in the records".[29] In addition, there is nothing to suggest that the IIO Lawyer's communications with the Director and the IIO staff during the course of his investigation were not kept private, so I also find that they were confidential communications. Therefore, I am satisfied that the information that reveals the content of the IIO Lawyer's investigation and communications regarding the privacy concern meets the criteria for legal advice privilege.[30]

[39] In summary, I find that all of the information withheld under s. 14 meets the criteria for protection under legal advice privilege.

Waiver

[40] I will briefly address the issue of waiver of privilege, which is raised by the IIO.

[41] Waiver of privilege is ordinarily established where it is shown that the possessor of the privilege knows of the existence of the privilege and voluntarily shows an intention to waive that privilege.[31] The law is well established that the privilege belongs to, and may only be waived by, the client. In addition, once solicitor client privilege is established, the onus of showing it has been waived is upon the party seeking to displace it.[32] The applicant in this case provides no submissions or evidence regarding waiver.

[42] The IIO says that it provided some of the privileged records to the OPCC in confidence for the purposes of the OPCC's investigation. The IIO submits,

---

[29] Director's affidavit #1, para. 41.
[30] Large set: pp. 7-30, 39-44 (duplicate at 62-67 and 419-424), 49 (duplicate at 404-5), 55, 163, 164-165, 416 and 426.
[31] *S & K Processors Ltd. v. Campbell Ave. Herring Producers Ltd*., 1983 CanLII 407 (BCSC) at para 6.
[32] *Le Soleil Hotel & Suites Ltd. v. Le Soleil Management Inc., 2007 BCSC 1420 at para. 22; Maximum Ventures Inc. v. de Graaf***,** 2007 BCSC 1215 at para. 40.

however, that this did not amount to a waiver of privilege.[33] The Director deposes:

> The documents that I provided to the OPCC were provided in confidence and there was no intent on my part to waive privilege. Evidence can be found in the Records that I provided them to the OPCC in confidence.
>
> I expected that the OPCC would maintain confidentiality and not disclose these documents further without the consent of IIO. I understood this to be the case from conversations I had with OPCC.[34]

[43] The IIO only identifies one specific record, which it says was included in the information it shared with the OPCC.[35] However, the content of some of the other records suggests that more than this one record was likely shared. It is not possible, in my view, to determine with sufficient precision which records in dispute in this inquiry were shared with the OPCC because there was no additional evidence clarifying this matter.

[44] Given the importance of the solicitor client privilege to the functioning of the legal system, evidence justifying a finding of waiver must be clear and unambiguous.[36] That kind of evidence is simply not present in this case. Therefore, I am not satisfied that the IIO waived privilege when it shared its records with the OPCC.

[45] **Summary s. 14** – I find that the IIO has established that legal advice privilege applies to all of the information it withheld under s. 14, and the IIO may refuse to disclose it to the applicant on that basis.

Disclosure harmful to law enforcement (s. 15)

[46] In its submissions, the IIO submits that ss. 15(1)(a), (c) and/or (d) apply to the information it is withholding under s. 15. However, the severing in the records only identifies that information was withheld under s. 15 in general, so there is no means to determine where exactly the IIO intended the specific s. 15 provisions to apply. Therefore, I have considered all the information labelled as s. 15 as being withheld under ss. 15(1)(a), (c) and (d).

[47] The parts of s. 15 relevant to this inquiry are as follows:

> 15(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

---

[33] IIO's initial submissions, paras. 6.49-6.55.
[34] Director's affidavit #1, paras. 50-51.
[35] Director's affidavit #1, para. 45. The record is in the large set: pp. 39-44 (duplicated at 62-67 and 419-24).
[36] *Maximum Ventures Inc. v. de Graaf***,** supra note 34, at para. 40.

> (a) harm a law enforcement matter,
> ...
> (c) harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement,
> (d) reveal the identity of a confidential source of law enforcement information,

[48] The meaning of the term "law enforcement" is also relevant, and Schedule 1 of FIPPA defines it as follows:

> "law enforcement" means
> (a) policing, including criminal intelligence operations,
> (b) investigations that lead or could lead to a penalty or sanction being imposed, or
> (c) proceedings that lead or could lead to a penalty or sanction being imposed;

[49] The Supreme Court of Canada in *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)* [37] said the following about the standard of proof for exceptions that use the language "reasonably be expected to harm":

> This Court in *Merck Frosst* adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in *Merck Frosst* emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground… This inquiry of course is contextual and how much evidence and the quality of evidence needed to meet this standard will ultimately depend on the nature of the issue and "inherent probabilities or improbabilities or the seriousness of the allegations or consequences": *Merck Frosst*, at para. 94, citing *F.H. v. McDougall*, 2008 SCC 53 (CanLII), [2008] 3 S.C.R. 41, at para. 40.

[50] Further, in *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner),* [38] Bracken, J. confirmed that it is the release of the information itself that must give rise to a reasonable expectation of harm, and that the burden rests with the public body to establish that the disclosure of the information in question could result in the identified harm.

[51] The IIO has primarily applied s. 15 to information related to the privacy concern. However, it has also applied it to withhold a small amount of information related to IIO's usual business of investigating police officer-related incidents of

[37] 2014 SCC 31 at para. 54.
[38] 2012 BCSC 875 at para. 43.

death or serious harm. I will deal with each separately below. However, I will not consider the IIO's application of s. 15 to information that I have already found may be withheld under ss. 13 or 14.

Application of s. 15 to information about the IIO's usual business

[52] The IIO is applying s. 15 to information that relates to the IIO's investigation of police related incidents of death or serious harm. The IIO submits that these investigations are "law enforcement" matters under FIPPA, and that disclosure of the information being withheld under s. 15 could harm such investigations. Specifically, it says:

> The IIO engages in investigations of officers where there have been officer related incidents of death or serious harm. These investigations are conducted in order to determine whether or not an officer may have committed an offence. Moreover, at the conclusion of an investigation, the matter may be referred by the IIO to crown counsel for prosecution of officers. Therefore, the IIO's investigations can lead to a penalty or sanction being imposed, namely a conviction of an officer. Given this, the IIO submits that its investigations can qualify as law enforcement.[39]

[53] Previous orders have found that in order for a public body's investigation to meet the definition of law enforcement in FIPPA, the public body must have a specific statutory authority or mandate to conduct the investigation and to impose sanctions or penalties.[40] Although the IIO does not specifically say so, it is evident that the IIO's statutory mandate to investigate such matters is found in Part 7.1 of the *Police Act*.[41] Part 7.1 also provides for a sanction or penalty. It states that if, after an investigation, the Director considers that an officer may have committed an offence under any enactment, including an enactment of Canada or another province, the Director must report the matter to Crown counsel. Therefore, I find that the IIO's investigations of officer-related incidents of death or serious harm qualify as "law enforcement" matters under s. 15 of FIPPA.

[54] *Harms under ss. 15(1)(a) and (c)* - The IIO submits that disclosure of the information it is withholding under s. 15 would harm its ongoing or future investigations and harm the effectiveness of investigative techniques because:

> ... an individual who was aware of this information could attempt to manipulate future investigations to better ensure their desired outcome. Disclosure of specific actions taken, directives, and other aspects of the

[39] IIO's February 10, 2016 submission, para. 3.31.
[40] Order 36-1995, [1995] B.C.I.P.C.D. No. 8, at p. 14; Order 00-52, 2000 CanLII 14417 (BCIPC); Order F15-26, 2015 BCIPC 23 (CanLII).
[41] *Police Act*, in particular ss. 38.02, 38.09, 38.10, 44 and 177.1.

> investigation would affect the integrity of these investigations thereby causing harm to IIO's current or ongoing investigations.
> …
>
> As well, the IIO submits that disclosure would harm the effectiveness of investigative techniques which are used by the IIO in investigations as these techniques could be rendered useless if known generally.[42]

[55] For his part, the applicant says:

> Although investigations undertaken by the IIO may be complex and time consuming, they are reactive and primarily involve gathering and reporting information. Certainly during my time with the IIO there were no investigative techniques employed outside the norm (routine).[43]

[56] The withheld information includes details about IIO staff being scheduled to travel and testify at coroner's inquests, as well as the names of deceased in those inquests.[44] It is not apparent - and the IIO does not explain - how disclosure of such administrative information about staff scheduling and business travel, or the name of the deceased in that context (especially as the names are already part of the coroner's public record) could reasonably be expected to cause the s. 15 harms alleged. Therefore, I find that this information may not be withheld under ss. 15(1)(a) or (c).

[57] There are a few instances where the withheld information is about general protocol and procedures for investigation and testifying at inquests.[45] There is also a small amount of information of a non-sensitive nature about investigations the applicant was working on when employed by the IIO.[46] The Director's evidence about the harm from disclosure of this type of information is as follows:

> I believe that disclosure of this information could reasonably be expected to harm subsequent law enforcement matters or harm IIO's investigative techniques as individuals would be made aware of the steps taken or techniques used by the IIO.
>
> In knowing this information, an individual could attempt to manipulate future investigations to better ensure their desired outcome. Consequently, I believe that disclosure of this information would allow individuals to affect the integrity of an IIO investigation.[47]

[42] IIO's February 10, 2016, submission, paras. 3.32 and 3.34.
[43] Applicant's February 23, 2016 submission, p. 2.
[44] Large set: pp. 138-39, 183, 247 and 248.
[45] Small set: pp. 22-26.
[46] Large set: pp. 171-73, 443 and 450.
[47] Director's affidavit #2, para.17-18.

[58] The IIO does not elaborate on the Director's assertion or explain how an individual having the actual information at issue here could manipulate future investigations to better ensure a desired outcome. There is simply not enough information provided for me to see any link between disclosure of this particular information and the harm the IIO anticipates. The withheld information reveals only obvious or common sense procedure and investigative steps. Therefore, I am not satisfied that disclosing such information could reasonably be expected to result in harm under ss. 15(1)(a) and (c), so the IIO may not refuse to disclose it under those exceptions.

[59] The Director also identifies another way in which he believes disclosure would cause harm. He says:

> Moreover, with respect to information relating to the [name of deceased] investigation and inquest, the IIO is aware that a civil action was initiated. However, the IIO is unaware of the status of this action. The IIO believes that disclosure of this information could harm any ongoing proceedings.[48]

[60] The IIO and the Director provide no further detail about this civil action or how disclosure of the information could reasonably be expected to harm it (or any other proceedings). Other than the instances where I can see this particular deceased's name in the records, it is not actually clear what information the Director means when he refers to "this information" in the quote above. Further, I note that the deceased's name is already publicly known in the context of the investigation and inquest mentioned in the quote above, so I do not see how its disclosure could result in any of the harms under s. 15. Therefore, the IIO may not withhold this information under s. 15.

[61] *Harm under s. 15(1)(d)* – The IIO provided no argument or evidence about how disclosure of the information that is about IIO's usual business could reasonably be expected to result in harm under s. 15(1)(d). Therefore, I find that this information may not be withheld under s. 15(1)(d).

Application of s. 15 to information about the privacy concern

[62] The balance of the information that the IIO is withholding under s. 15 relates to the IIO and OPCC investigation of the privacy concern.

[63] *Harm under s. 15(1)(d)* - The IIO submits that disclosure of the withheld information about the privacy concern would reveal the identity of confidential sources of law enforcement information, so s.15 (1)(d) applies.[49] It identifies

[48] Director's affidavit #2, para. 40.

[49] IIO's initial submissions, paras. 6.58-6.62. The IIO does not identify where precisely it relied s. 15(1)(d). However it identifies by name the individuals who it says are the confidential sources, so I assume that s. 15(1)(d) was applied to their names.

several individuals who it says provided information during the IIO and OPCC investigations of the privacy concern.

[64] The first step in analyzing s. 15(1)(d) is to determine whether the information these individuals provided during those investigations qualifies as "law enforcement information" for the purposes of s. 15 (1)(d). Therefore, I have considered what the IIO's submissions and evidence reveal about whether these two investigations meet the definition of law enforcement in FIPPA (*i.e.*, policing, including criminal intelligence operations; investigations that lead or could lead to a penalty or sanction being imposed; or proceedings that lead or could lead to a penalty or sanction being imposed).

[65] The IIO's description of the investigations is as follows:

> A workplace investigation was commenced with respect to the privacy breach and a further investigation was then undertaken with respect to particular employees at the IIO. The investigation into the IIO employees had the potential to lead to a penalty or sanction being imposed – namely employee discipline, suspensions, or terminations.[50]

[66] The Director's letter to the OPCC asking for help said the following:

> I require the assistance of the OPCC to determine the full extent of the privacy breach and to specifically identify any IIO investigator who has either lied or participated in a breach of trust to cover up misconduct relating to the privacy breach. Although the privacy breach was minor and determined by myself likely not to require a disciplinary response (assuming no IIO supervisor was aware or took part in the conduct), any acts taken to cover up participation in such a breach cuts to the very integrity of the IIO program and requires a swift and strong response. "Code of silence" type values cannot be tolerated to be part of the developing IIO culture and are contrary to my early instructions to staff and to our developing Mission, Vision and Values.[51]

[67] The IIO says that it engaged the OPCC to act on its behalf and investigate as the IIO's agent. The Director says, "The IIO has policy with respect to when it will turn over investigations to the OPCC. That policy was followed here."[52] However, the IIO did not provide any further detail or a copy of the policy.

[68] As already mentioned above, in previous BC Orders where s. 15(1) was found to apply, the information at issue related to investigations, proceedings,

---

[50] IIO initial submissions, para. 6.59.
[51] Large set: p. 47 (large set). This portion of the letter has already been disclosed to the applicant.
[52] Director's affidavit #1, para. 47.

penalties and sanctions that were authorized by statute.[53] I have carefully reviewed the IIO's submissions and evidence and the records in dispute, but I can find no reference to any statute or regulation as being the source of either the IIO or the OPCC's authority to investigate the privacy concern and related employee conduct.

[69] I have considered the *Police Act* and whether it applies to the investigations at issue in this case. Part 11 deals with misconduct, complaints, investigations and discipline matters related to members and former members. Based on the definitions of "member" and "former member" in Part 11, and what Part 7.1 says about who may be appointed as an IIO investigator, it does not appear that the investigations in this case took place under Part 11.[54] Therefore, it does not appear that the IIO's or the OPCC's investigations were conducted under the *Police Act*.

[70] The *Police Act* (s. 38.06) states that the appointment of IIO investigators must be in accordance with the *Public Service Act*, so I also considered that statute. However, there is nothing that I can see in the *Public Service Act* about privacy breaches or the employee conduct at issue here. Therefore, in my view, the IIO's or the OPCC's investigations were not conducted under the *Public Service Act* either.

[71] In conclusion, there is no evidence of a statute authorizing, or being enforced by, the IIO and the OPCC investigations of the privacy concern and employee conduct. Therefore, I am not satisfied that those investigations meet the definition of "law enforcement" for the purposes of s. 15. It follows, therefore, that the individuals who provided information for those investigations were not a source (confidential or otherwise) of "law enforcement" information under s. 15(1)(d).

[72] *Harm under s. 15(1)(a)* - The IIO also submits that disclosure of the withheld information about the privacy concern would harm "ongoing" investigations.[55] However, it does not identify any ongoing investigations. I presume it does not mean the privacy concern investigations because the evidence and records in dispute establish that they are long since concluded. Further, the IIO provides no argument or evidence to suggest that it means that disclosure of the privacy concern information relates in any way to the IIO's investigations of police related incidents of death or serious harm.

---

[53] For example: Order F15-26, supra note 40 (*Environmental Management Act*); Order 00-52, supra note 40 (*Securities Act*); Order 00-18, 2000 CanLII 7416 (BCIPC) (*Motor Vehicle Act*); Order 00-01, 2000 CanLII 9670 (BCIPC) (bylaws enacted under the *Municipal Act*).

[54] Further, it does not appear that the behaviour under investigation in this case even meets the definition of "misconduct" in Part 11.

[55] IIO initial submissions, para. 6.63.

[73] Since the IIO has not explained what the "ongoing" investigations are, I am unable to determine if they are "law enforcement" matters for the purpose of s. 15. Moreover, the IIO did not explain the nature of the harm it fears or how disclosure of the information at issue could reasonably be expected to cause harm to those unspecified ongoing matters. Therefore, I find that the IIO has not established that disclosure of the information about the privacy concern, which is being withheld under s. 15, could reasonably be expected to harm a law enforcement matter under s. 15(1)(a).

[74] *Harm under ss. 15(1)(c)* - The IIO also submits that disclosure of the withheld information about the privacy concern would harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement.[56] The Director's evidence about the techniques used by the IIO in investigating the privacy concern and the harm he believes would flow from disclosure is provided *in camera.*[57]

[75] The applicant submits that s. 15 only applies to techniques that are not generally known to the public. He says that the investigative techniques employed in the investigations of the privacy concern matter were common and routine, such as interviewing employees and examining his workstation computer, cell phone and flash drives seized from his work station.[58]

[76] In my view, the investigative techniques that the IIO wishes to keep secret are obvious and clearly known to the general public. Given this, the potential for the information to be used in the way the IIO anticipates already exists and would not flow from disclosure of the specific information at issue here. In my view, the IIO has not established that disclosure in this instance could reasonably be expected to harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement. Therefore, the information may not be withheld under s. 15(1)(c).

[77] **Summary s. 15** - In summary, I find that the IIO has not established that disclosure of the withheld information could reasonably be expected to cause harm under ss. 15(1)(a),(c) and (d). Therefore, the IIO is not authorized to refuse to disclose that information to the applicant under those exceptions. However, much of this information is also being withheld under s. 22, so I will address it again below when I consider that exception.

Disclosure Harmful to Intergovernmental Relations (s. 16)

[78] The IIO is withholding a small amount of information under s. 16(1)(b), which states as follows:

---

[56] IIO initial submissions, paras. 6.63 and 6.64.
[57] Director's affidavit #1, paras. 64-65.
[58] Applicant's April 17, 2015 submission, para. 111.

> 16(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 the conduct by the government of British Columbia of relations between that government and any of the following or their agencies:
>
> (i) the government of Canada or a province of Canada;
>
> …
>
> (b) reveal information received in confidence from a government, council or organization listed in paragraph (a) or their agencies …

[79] Section 16(1)(b) requires a public body to establish that disclosure would reveal information received from a government, council or organization listed in s. 16(1)(a) or one of their agencies, and that the information was received in confidence.[59]

[80] The IIO submits that s. 16(1)(b) applies to several excerpts in the records because disclosure would reveal information received in confidence from the RCMP. The applicant submits that if the information refers to him, then it should be disclosed to him. I have reviewed the information and none of it refers to the applicant. The information being withheld under s. 16 is a reference to an RCMP file in a log of investigative materials found at the applicant's former workstation, two RCMP inspectors' cellphone numbers, and two handwritten notes referring to police matters.

[81] Based on the affidavit evidence of the Director and the content and context of the information, I am satisfied that the information withheld under s. 16 was received from the RCMP, which is an agency of the government of Canada for the purpose of s. 16(1)(b).[60]

[82] With regards to confidentiality, the IIO submits that it has entered into a "Memorandum of Understanding Respecting Investigations" with the RCMP and BC's municipal police departments. A copy of the memorandum was not provided, and there is no mention of its date. However, I am satisfied that this is the type of governing document that would have been entered into in the earliest stages of the IIO's existence, so the statements it contains about confidentiality were applicable at the time the information in dispute here was created. The Director deposes that the memorandum says the following about confidentiality:

> …the IIO and police services shall: (a) use on another's records and information solely for purpose of investigations within their respective jurisdictions; (b) for the purposes of section 13(1) of the *Access to*

[59] Order 02-19, 2002 CanLII 42444 (BC IPC), para. 18.
[60] For similar finding see: Order 02-19, ibid, and Order F11-06, 2011 BCIPC 7 (CanLII).

> *Information Act* (Canada), section 19(1)(a) of the *Privacy Act* (Canada), and sections 16(1)(b) and 16(2) of the *Freedom of Information and Protection of Privacy Act* (British Columbia), treat all records and information relating to IIO investigations as confidential and not to be disclosed to third parties except with written consent of the originating service and the Attorney General, or as otherwise required by law....[61]

[83] The Director also says that he believes that disclosure of the s. 16 Information could reasonably be expected to reveal information received in confidence from the RCMP.[62]

[84] For information to have been "received in confidence" there must be an implicit or explicit agreement or understanding of confidentiality on the part of both those supplying and receiving the information.[63] The IIO's evidence regarding the Memorandum of Understanding satisfies me that the information in dispute in this case was received from the RCMP in confidence.

[85] **Summary s. 16(1)(b)** – I find that disclosure of the information being withheld under s. 16 would reveal information received in confidence from the RCMP, which is an agency of the government of Canada. Therefore, the IIO has established that it may refuse to disclose to the applicant the information it withheld under s. 16(1)(b).[64]

Disclosure harmful to personal privacy (s. 22)

[86] The IIO is refusing to disclose some information to the applicant on the basis that disclosure would be an unreasonable invasion of third party personal privacy under s. 22. It submits that it is the personal information of third parties, and it is not the applicant's personal information. The applicant submits that only third party personal information such as addresses, phone numbers and dates of birth should be withheld from the records. Numerous orders have considered the application of s. 22, and I will apply those same principles in my analysis.[65]

Personal information

[87] The first step in any s. 22 analysis is to determine if the information is personal information. Personal information is defined as **"**recorded information about an identifiable individual other than contact information". Contact information is defined as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business

[61] Director's affidavit #2, para. 22.
[62] Director's affidavit #1, para. 68 and affidavit #2, paras. 24 and 44.
[63] Order 331-1999, 1999 CanLII 4253 (BCIPC) at pp.6-9.
[64] Large set: pp. 256, 444 and 466 and small set: pp. 21 and 37.
[65] See for example, Order 01-53, supra note 22, p. 7.

telephone number, business address, business email or business fax number of the individual".[66]

[88] I have reviewed the records and find that the information withheld under s. 22 is personal information. In addition, there is some information that I determined could not be withheld under s. 15 that is also personal information.[67] The IIO did not apply s. 22 to that information, but I will consider it here because s. 22 is a mandatory provision.

[89] The personal information is comprised of third parties names and other information that would easily allow the applicant to identify the third parties given the context and the fact that he worked at the IIO. Some of the information is about what third parties observed of the applicant's actions and conduct and how they responded and interacted with him. I find that it is a mix of both the third parties' and the applicant's personal information. There is also some personal information about a named third party's death (compiled in the course of the IIO's operational mandate).

Section 22(4)

[90] The next step in the s. 22 analysis is to determine if the personal information falls into any of the types of information listed in s. 22(4). If it does, then disclosure would not be an unreasonable invasion of personal privacy. The IIO submits that none of the subsections in s. 22(4) apply to the personal information in this case. I agree.

Presumptions

[91] The third step is to determine whether any of the presumptions in s. 22(3) apply, in which case disclosure is presumed to be an unreasonable invasion of third party privacy. For the information that I am considering under s. 22 (*i.e.*, which I have not already found may be withheld under another exception), the relevant presumptions are as follows:

> 22(3) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if
>
> …
>
> (b) the personal information was compiled and is identifiable as part of an investigation into a possible violation of law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation,
>
> …
>
> (d) the personal information relates to employment, occupational or educational history,

[66] See Schedule 1 of FIPPA for these definitions.

[67] Large set: 33, 39, 51, 52, 53, 55, 56, 232-41 and 352-53.

> …
> (g) the personal information consists of personal recommendations or evaluations, character references or personnel evaluations about the third party,

[92] *Section 22(3)(b)* - The IIO submits that s. 22(3)(b) applies to a portion of the personal information because it relates to an IIO investigation into police officer involvement in incidents of serious harm or death. The IIO says it is clear that the information was compiled, and is identifiable, as part of an investigation into a possible violation of the law. I agree with the IIO's characterization of this information and find that it relates to the IIO's operational mandate to investigate incidents of serious harm and death involving police officers and the RCMP in BC. Disclosure of such information is presumed, under s. 22(3)(b), to be an unreasonable invasion of the personal privacy of the third parties identified.

[93] *Section 22(3)(d)* - The IIO also submits that s. 22(3)(d) applies because some of the personal information is about the employment, occupational or educational history of third parties. Specifically, it submits that this information includes the names of job applicants, their qualifications and résumés, information about their job interviews and how they did in job competitions. The Director deposes that some of the information also contains employment disciplinary information with respect to third parties.

[94] I find that s. 22(3)(d) applies to most of the personal information. For instance, the personal information about third party employees' educational and employment history in the context of job applications (*i.e.*, in résumés, job competition scores, interview results, reference checks). It also applies to several instances of personal information about existing employee training progress and work development, as well as details about job offers. I also find that s. 22(3)(d) applies to third parties' names and other identifying information where it appears in the context of the workplace investigation into the privacy concern and the third parties' actions and conduct. Previous orders have consistently found s. 22(3)(d) applies to this type of third party personal information when it relates to an investigation into workplace disciplinary matters.[68] Further, s. 22(3)(d) applies to some information that reveals workplace discipline or sanctions imposed on third parties.[69]

[95] *Section 22(3)(g)* - The IIO also submits that s. 22(3)(g) applies because some of the personal information consists of evaluations and ranking of candidates who participated in a job competition, as well as what reference checks revealed. I agree and find that there is some personal information of this type and that s. 22(3)(g) applies to it as well as s. 22(3)(d).

---

[68] Order 01-53, supra note 22, para. 40.
[69] For a like finding, see Order F08-08, 2008 CanLII 21700 (BCIPC).

[96] In addition, consistent with previous orders,[70] I find that s. 22(3)(g) applies to the investigators' evaluative comments of the third parties' behaviour and responses during the investigation.

[97] In conclusion, I find that ss. 22(3)(b),(d) and (g) apply to the majority of the personal information. However, there are some instances where no presumptions apply, for example where the personal information is about employees' personal lives and personal contact information.

Relevant circumstances – Section 22(2)

[98] The final step in the s. 22 analysis is to consider the impact of disclosure of the personal information in light of all relevant circumstances, including those listed in s. 22(2). It is at this step that the ss. 22(3)(b),(d) and (g) presumptions may be rebutted. The applicant makes no submissions regarding relevant factors. The IIO says that it considered relevant circumstances, in particular s. 22(2)(f), and determined that there were no factors that would favour disclosure of the personal information. Section 22(2)(f) states:

> 22 (2) In determining under subsection (1) or (3) 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
> …
> (f) the personal information has been supplied in confidence,
> …

[99] The IIO submits that much of the personal information, including that related to the workplace investigation, would have been provided with expectation of privacy.[71] This, it says, favours a finding that disclosure would be an unreasonable invasion of personal privacy.

[100] There is no evidence before me that the résumés and other information provided by job applicants and those assessing them (i.e., interview results, interviewers' evaluative comments, references, job offers, etc.) were submitted explicitly in confidence. However, I agree with previous orders, which have found that résumé and job application information is typically supplied with the implied understanding that it, and any assessment of the candidate, is confidential and will be treated as such by the employer.[72] The same confidentiality applies, in my view, to information about existing employee progress in training and work development matters. I therefore find that s. 22(2)(f) weighs in favour of withholding such information.

---

[70] See for example, Order 01-07, 2001 CanLII 21561 (BC IPC) at para. 21; Order F14-10, 2014 BCIPC 12 (CanLII) at para. 19.
[71] IIO's February 10, 2016 submission, para. 3.60.
[72] See, for example, Order F14-41, 2014 BCIPC 44.

[101] I also find that s. 22(2)(f) favours withholding the personal information about the workplace investigation.[73] Typically, information that is provided by witnesses during a workplace investigation is supplied in confidence. There is nothing to suggest that this was not the case here. Further, the actual content of that information supports a finding that it was intended by the individual communicating it to be held in confidence.

[102] *Other relevant circumstances* - The IIO acknowledges that the applicant likely has some knowledge of the personal information related to the privacy concern investigations. However, the IIO submits that this prior knowledge does not warrant disclosure. In addition, the IIO says that it considered the fact that the OPCC disclosed some of the personal information at issue to the applicant, but it did not follow suit because it determined that this was not authorized under s. 22.

[103] It is apparent from the applicant's submissions, that given his own involvement in the privacy concern, he is already familiar with some of the specific content of the withheld information. He also states that he received some information about that matter directly from the OPCC in response to his access request to the OPCC. It is also likely that he is familiar with some of the personal information related to matters the IIO investigated under its operational mandate involving third party deaths. The applicant may even have investigated some of those cases when employed by the IIO.

[104] In my view, the possibility that the applicant may have existing knowledge of some of the personal information because the OPCC disclosed it to him does not weigh strongly in favour of disclosure here. Neither party provided specifics about what, if anything, the OPCC may have severed from the records it disclosed, so it is unclear if the specific information at issue in this inquiry has already been disclosed by the OPCC.

[105] Further, the applicant's general understanding of the privacy concern investigation and the individuals involved, as well as his knowledge of cases he worked on when employed by the IIO are not sufficient reasons, in this case, to disclose such third party personal information. It is sensitive information of the type generally supplied and gathered in confidence, and while the applicant has expressed no plans to disseminate the information further, I recognize that disclosure to an applicant is, in essence, disclosure to the world, and FIPPA places no restrictions on what an applicant may do with information he or she receives [74]

[73] See, for example, Order 01-07, supra note 70, and Order F08-02, 2008 CanLII 1645 (BC IPC).
[74] Order 03-35, 2003 CanLII 49214 (BCIPC), at para. 31.

[106] In conclusion, considering all relevant factors including those in s. 22(2), I find that the ss. 22(3)(b),(d) and (g) presumptions have not been rebutted.

[107] Furthermore, I can see no circumstances that weigh in favour of disclosing the personal information that is not protected by the presumptions. It is about third parties' personal lives, activities and contact details, and it does not reflect in any way on their work activities related to the applicant and the IIO. I also note that the applicant says that he has no interest in information related to such matters.[75] Therefore, I find that its disclosure, in this case, would be an unreasonable invasion of third party personal privacy.

Severing under s. 4(2)

[108] Some of the witness statements and evaluative statements of investigators and other third parties are about the applicant. Thus, the information is the personal information of the applicant as well as the personal information of the third party. Section 4(2) of FIPPA states that, where it is reasonable to sever excepted information from a record, an applicant has the right of access to the remainder.

[109] Previous orders have considered the issue of joint or "inextricably intertwined" personal information and have generally found that it is not reasonable to separate an applicant's personal information from a third party's personal information in such instances.[76] I find that to be the case here, as the withheld information about the applicant is so intertwined with the personal information of the third parties that severing is not reasonable under s. 4(2).

Section 22(5) summary

[110] A public body must create a summary of an applicant's personal information pursuant to s. 22(5) of FIPPA, unless the summary cannot be prepared without revealing the identity of a third party who provided the information in confidence. In this case, the IIO is withholding the witness statements and evaluative comments and opinions about the applicant expressed by others during the workplace investigation. In my view, given the applicant's knowledge of the events and the individuals involved, a summary of this information cannot be made without revealing to him the third parties' identities.

[111] **Summary s. 22** – I find that the IIO must continue to refuse to disclose to the applicant the personal information it is withholding under s. 22(1). The presumptions in ss. 22(3)(b),(d) and (g) apply to much of it, and after considering all relevant circumstances, I find that the presumptions have not

[75] Applicant's February 23, 2016 submission.
[76] See, for example: Order F14-10, supra note 70; Order F08-02, supra note 73.

been rebutted. In addition, after considering all relevant circumstances, I also find that disclosure of the personal information that is not covered by a presumption would also be an unreasonable invasion of third party personal privacy under s. 22(1).

CONCLUSION

[112] For the reasons above, I make the following order under s. 58 of FIPPA:

1. I confirm the IIO's decision to refuse to give the applicant access to records because they are outside the scope of FIPPA pursuant to s. 3(1)(c).

2. I confirm the IIO's decision to refuse to give the applicant access to information under ss. 13, 14 and 16.

3. The IIO is not authorized to refuse to give the applicant access to information under s. 15. I require the IIO to give the applicant access to that information, unless it is withheld under s. 14 or s. 22 in compliance with this order.

4. The IIO is required under s. 22 to refuse to give the applicant access to all of the third party personal information in the records. This includes the personal information highlighted in orange on pages 33, 39, 51, 52, 53, 55, 56, 232-41 and 352-53 (large set). A copy of the pages with the orange highlighting is being sent to the IIO along with this order.

5. The IIO must comply with this Order on or before **July 21, 2016.** The IIO must concurrently copy the OIPC's Registrar of Inquiries on its cover letter to the applicant, together with a copy of the records.

June 8, 2016

ORIGINAL SIGNED BY

Elizabeth Barker, Senior Adjudicator

OIPC File No.: F14-58798