Order F25-24

MINISTRY OF PUBLIC SAFETY AND SOLICITOR GENERAL

Allison J. Shamas
Adjudicator

March 26, 2025

CanLII Cite: 2025 BCIPC 30
Quicklaw Cite: [2025] B.C.I.P.C.D. No. 30

Summary: An applicant asked the Ministry of Public Safety and Solicitor General (Ministry) for access to records about them in the custody and control of the Crime Victim Assistance Program. The Ministry took the position that some records were outside the scope of the *Freedom of Information and Protection of Privacy Act* (FIPPA) by operation of s. 3(3)(f) (records created for an officer of the Legislature) and withheld information from those and other records under various exceptions to disclosure under FIPPA. The adjudicator confirmed the Ministry's decision under s. 3(3)(f) in full, its decision under s. 13(1) (advice and recommendations) in part, but held that it was not required to withhold any of the information at issue under s. 22(1) (unreasonable invasion of personal privacy). The adjudicator also found that the Ministry had not properly exercised its discretion under s. 13(1). As a result, the adjudicator ordered the Ministry to disclose the information it was not authorized or required to withhold under ss. 13(1) and 22(1), and to reconsider its decision to withhold the information to which s. 13(1) applied, and in doing so to exercise its discretion upon proper considerations.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, ss. 3(3)(f), 13(1), 13(2), 13(3), 22(1), 22(2)(a), 22(2)(c), 22(2)(e), 22(2)(h), 22(3)(b), 22(3)(d), 22(4)(c), and 22(4)(e), and Schedule 1 (Definition of "officer of the Legislature").

INTRODUCTION

[1] An individual (applicant) asked the Ministry of Public Safety and Solicitor General (Ministry) for access to records related to her in the custody and control of the Crime Victim Assistance Program (CVAP).

[2] The Ministry provided the applicant with some of the requested records but took the position that three records were outside the scope of the *Freedom of Information and Protection of Privacy Ac*t (FIPPA) by operation of s. 3(3)(f) (records created for an officer of the Legislature) and withheld information from those and other records under ss. 13(1) (advice and recommendations), 15

(disclosure harmful to law enforcement), 16 (disclosure harmful to intergovernmental relations or negotiations), and s. 22(1) (unreasonable invasion of third-party personal privacy) of FIPPA.

[3] The applicant asked the Office of the Information and Privacy Commissioner (OIPC) to review the Ministry's decision.

[4] During the OIPC's mediation process, the Ministry reconsidered its initial severing decisions. It withdrew its reliance on ss. 15 and 16 of FIPPA and provided the applicant with access to information that it previously withheld under ss. 13(1) and 22(1).

[5] Mediation did not resolve the balance of the issues in dispute, and the matter proceeded to inquiry.

[6] Prior to the inquiry process, the applicant withdrew her request for access to a telephone number prefix. In addition, during the inquiry the applicant withdrew her request for information the Ministry described as personal information about a third party's family member.[1] As the applicant is no longer seeking access to this information, it is no longer in dispute, and I will not consider it further.[2]

[7] During the inquiry, I determined two CVAP employees were appropriate persons within the meaning of s. 54(b) of FIPPA. I invited those employees to provide submissions on s. 22(1) and both employees made submissions. In deciding the issues in dispute, I have considered the submissions made by all four parties to the inquiry.

ISSUES AND BURDEN OF PROOF

[8] The issues I must decide in this inquiry are:

1. Are some of the records requested by the applicant excluded from the scope of FIPPA under s. 3(3)(f)?
2. Is the Ministry authorized to refuse to disclose the information in dispute under s. 13(1)?
3. Is the Ministry required to refuse to disclose the information in dispute under s. 22(1)?

[1] Paragraph 6 of the OIPC Fact Report, paragraph 65 of the Ministry's submission, and paragraph 7 of the applicant's submission.
[2] The information that is no longer in dispute is found on pages 81, 84, 88, 92, and 107 of the records.

[9] It is well-established that the public body has the burden of establishing that records are excluded from the scope of FIPPA, including under s. 3(3)(f).[3] As for the exceptions to disclosure, s. 57(1) of FIPPA places the burden on the Ministry to prove the applicant has no right of access to the information withheld under s. 13(1), and s. 57(2) places the burden on the applicant to prove that disclosure of any personal information would not be an unreasonable invasion of a third party's personal privacy under s. 22(1). However, under s. 22(1), the Ministry has the initial burden of proving the information at issue is personal information.[4]

BACKGROUND

[10] In her access request, the applicant seeks information about an incident in which her information was improperly accessed and viewed by a CVAP employee.[5]

[11] CVAP is a government run program operated by the Ministry that provides financial benefits to victims of crime.[6]

[12] In 2022, the applicant applied to CVAP for benefits. Based on the information the applicant provided, and the police records CVAP collected to adjudicate the applicant's claim, CVAP determined that the applicant was a victim of crimes and was eligible for benefits.[7]

[13] On August 19, 2022, one CVAP employee (Employee 1) disclosed information about the applicant's claim to another CVAP employee (Employee 2). Employees 1 and 2 (collectively referred to as the Employees) are the appropriate persons who were added as parties to this inquiry. Following Employee 1's disclosure, Employee 2 accessed and viewed the applicant's file without any business purpose for doing so (the privacy incident).[8] Also on August 19, 2022, Employee 1 informed their supervisor that they had disclosed information about the applicant's file to Employee 2.

---

[3] See for example Order F23-109, 2023 BCIPC 125 (CanLII) at para 5; Order F23-08, 2023 BCIPC 10 (CanLII) at para 6; Order F15-26, 2015 BCIPC 28 (CanLII) at para 5; and Order 03-06, 2003 CanLII 49170 (BC IPC) at para 6.

[4] Order 03-41, 2003 CanLII 49220 (BCIPC) at paras 9-11.

[5] Ministry initial submission at para 19. OIPC Investigator's decision letter dated February 2, 2023, applicant's initial submission, tab 2, affidavit of applicant, exhibit O.

[6] Ministry initial submission, tab 2, affidavit of CVAP Director at para 1.

[7] Records p 14. I will use the terms "crime" going forward because in this case both the applicant and the Ministry agree that the applicant was a victim of a crime.

[8] Except as otherwise indicated, the events described in paras 11-19 are found in paras 16-26 of the Ministry's initial submission. The applicant agrees that those facts are accurate (para 2 of the applicant's response submission). The appropriate persons do not take issue with the Ministry's version of events.

[14] On or about August 23, 2022, CVAP and/or the Ministry sought advice from the provincial government's Office of the Chief Information Officer (CIO) about how to address the incident and fulfill its notification obligations to the applicant. A CIO employee (the CIO Employee) was assigned to the file.

[15] The Director of CVAP (CVAP Director or Director) notified the applicant of the incident by phone on November 8, 2022, and sent the applicant a formal written notification of the breach on November 18, 2022. The written notification informed the applicant that on August 19, 2022, their name, application to CVAP, and police records were "inappropriately accessed by a government employee;" that CVAP had investigated the issue and would take steps to address the incident; and that at that time CVAP had no reason to believe anything improper was or would be done with the applicant's personal information.[9] However, citing privacy concerns, the Director did not reveal the name of the employees involved.

[16] The applicant states that a family member of the person who committed the crimes against her (the accused)[10] worked at CVAP at the time of the incident, and that in the 10 days following the breach, the accused began behaving in a threatening manner and referencing the police report that was part of the applicant's file. The applicant also states that she suspects that Employee2 is that family member, and that the trigger for the accused's conduct around that time was that Employee 2 disclosed information from her file to the accused.

[17] In 2022, the applicant filed a complaint with the OIPC alleging that the Ministry used her personal information contrary to s. 32 of FIPPA and failed to protect her privacy as required by s. 30 of FIPPA (the OIPC Privacy Complaint). An OIPC Investigator (OIPC Investigator) found that both claims were substantiated.[11]

[18] In 2023, the applicant requested the OIPC review the Ministry's response to the access request that is at issue in this inquiry.[12]

[19] In 2024, the applicant filed a notice of civil claim (Notice of Claim) against the Minister of Public Safety and Solicitor General (Minister), CVAP Director, and five unnamed CVAP employees alleging negligence and breaches of *FIPPA* and the *Privacy Act*[13] (the Civil Claim).[14]

---

[9] Records p 105.
[10] I use the term "accused" because both the applicant and the Ministry agree that this individual committed crimes against the applicant.
[11] OIPC Investigator's letter of February 2, 2023, applicant's initial submission, tab 2, affidavit of applicant, exhibit O.
[12] OIPC Fact Report.
[13] RSBC 1996, c 373.
[14] Notice of Claim in the Civil Claim, applicant's initial submission, tab 2, affidavit of applicant, exhibit A (Notice of Claim).

[20] It is against this backdrop that the applicant requests access to records.

RECORDS IN DISPUTE

[21] The responsive records consist of email messages and documents related to the applicant's application to CVAP, the privacy incident, and the Ministry's response to the privacy incident including the involvement of the CIO Employee and the OIPC Investigator.

[22] There are 151 pages in total and the Ministry withheld information from nine on the basis that the information is outside the scope of FIPPA under s. 3(3)(f) and withheld 18 additional pages in full or in part under ss. 13(1) and 22(1) of FIPPA.

RECORDS THAT RELATE TO THE EXERCISE OF FUNCTIONS OF AN OFFICER OF THE LEGISLATURE UNDER AN ACT – S. 3(3)(F)

[23] Section 3(3)(f) provides that FIPPA does not apply to "a record that is created by or for, or that is in the custody or control of, an officer of the Legislature and that relates to the exercise of functions under an Act."

[24] Section 3(3)(f) replaces the former s. 3(1)(c). The wording of these two sections is substantially the same – the only change to s. 3(3)(f) was to delete the words "that officer's" before the word *functions*.[15] In a recent order, the OIPC held that orders considering the former s. 3(1)(c) remain persuasive in interpreting s. 3(3)(f).[16] Given the substantially similar language, I agree.

[25] For s. 3(3)(f) to apply, the following three 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 functions under an Act.[17]

---

[15] The former s. 3(1)(c) provided that FIPPA did not apply to "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."
[16] Order F23-109, 2023 BCIPC 125 (CanLII) at para 50.
[17] I note that this is substantially the same test as that defined in Order F16-28, 2016 BCIPC 30 (CanLII) at para 16, modified to account for the new language.

Parties' submissions

[26] The Ministry takes the position that s. 3(3)(f) applies to some of the information in two email chains and a document titled incident summary.[18] The Ministry states it withheld questions posed by the OIPC Investigator assigned to investigate the applicant's OIPC Privacy Complaint and the Ministry's responses to those questions from these records. It further explains that it prepared the responses for the purpose of assisting the OIPC Investigator to carry out their investigation into the incident.

[27] In support of its position, the Ministry submits that s. 3(3)(f) applies to a public body's internal records created for an OIPC investigation or review, such as a memorandum about an OIPC investigation. The Ministry further submits that the Information and Privacy Commissioner (Commissioner) is an officer of the Legislature pursuant to schedule 1 of FIPPA, and that conducting investigations to ensure compliance with *FIPPA* is one of the Commissioner's statutory functions.

[28] The applicant did not address s. 3(3)(f).

Findings and analysis – s. 3(3)(f)

[29] The records at issue are emails between the CVAP Director and the CIO Employee and a document titled "incident summary." The Ministry disclosed some of the information in these records.[19] In the parts of the records the Ministry disclosed, the Director tells the CIO Employee that the OIPC Investigator has questions about the privacy incident and asks the CIO Employee for assistance answering the questions. The Ministry withheld the OIPC Investigator's list of questions, as well as discussions about, draft, and final responses to those same questions from emails between the Director and CIO Employee and the incident summary document.

[30] For the reasons below, I am persuaded that these records satisfy the criteria required to engage s. 3(3)(f).

Officer of the Legislature

[31] Schedule 1 of FIPPA defines an "officer of the Legislature" to include "the Information and Privacy Commissioner."[20] In addition, it is well established that the term "officer of the Legislature" includes the officer's staff who are carrying

[18] The Ministry withheld information from the pp 71-73, 75-76, and 122-125 of the records under s. 3(3)(f).
[19] Section 3(3)(f) applies to entire records, not to information. While the Ministry withheld only certain information in considering the application of s. 3(3)(f), I have considered the records in the entirety, not just the information that the Ministry withheld.
[20] See also Order 03-44, 2003 CanLII 49223 (BC IPC) at para 22.

out statutory powers and duties on behalf of the officer.[21] Therefore, I find the involvement of an OIPC Investigator who is the Commissioner's delegate, satisfies the first requirement.

Created by or for the officer of the Legislature, or in the officer's custody or control

[32] The Ministry did not argue that the records were "created by" or are "in the custody or control" of the OIPC Investigator. Therefore, the only question is whether the records were "created for" the OIPC Investigator.

[33] It is clear from the content of the records that the CVAP Director and the CIO Employee drafted the emails and document during the OIPC's Investigation of the OIPC Privacy Complaint, and for the purpose of responding to the OIPC Investigator's questions.

[34] While it is not clear whether the records were ever sent to the OIPC Investigator, previous orders interpreting s. 3(1)(c) have clarified that the provision does not require records to be sent to or from an officer to satisfy the test.[22] Rather, what is required is that the internal records were created as a result of the officer's involvement. In this regard, in past orders, OIPC adjudicators have found that the following records were records "created for" an officer of the Legislature: handwritten notes and internal memoranda prepared by a public body during an investigation by an officer;[23] draft submissions created for an application to the OIPC;[24] and internal emails drafted by public body employees to discuss how to address or respond to the issue raised by an officer.[25]

[35] The nine pages of records at issue are internal emails and document that discuss how to respond to the OIPC's Investigator's questions. Consistent with past orders, I find that these records meet the second criterion for s. 3(3)(f) to apply because they were clearly created for the Commissioner's delegate as a direct result of the OIPC's investigation into the applicant's OIPC Privacy Complaint.

Related to the exercise of functions under an Act

[36] I also find that the records relate to the exercise of functions under FIPPA. Section 42(2)(a) authorizes the Commissioner (or their delegate) to "investigate

---

[21] See for example Order F06-06, 2006 CanLII 32975 (BC IPC) at para 5 and the cases cited therein.
[22] Order 01-43, 2001 CanLII 21597 at paras 13-14; Order 02-12, 2002 CanLII 42437; Decision F06-06, 2006 CanLII 32975; and Order F13-01, 2013 BCIPC 13 (CanLII) at para 15.
[23] Order 01-43, 2001 CanLII 21597, at paras 39–41.
[24] Order F13-01, 2013 BCIPC 13 (CanLII) at paras 9, 15 and 16.
[25] Order F21-39, 2021 BCIPC 47 (CanLII) at paras 18 and 21.

and attempt to resolve complaints that a duty imposed under [FIPPA] has not been performed." The records were created during and for the purpose of the OIPC's Investigation into the applicant's complaint that the Ministry breached FIPPA. Therefore, I find the records clearly relate to the exercise of statutory functions under FIPPA.

Conclusion – s. 3(3)(f)

[37] I find that s. 3(3)(f) applies to the nine pages of records at issue under that provision.[26] As a result, these records are outside the scope of FIPPA, and the applicant has no right of access to them under FIPPA.

[38] I will now consider the Ministry's application of ss. 13(1) and 22(1) to the information the Ministry withheld from the remaining 18 pages of records in dispute.

SECTION 13(1) – ADVICE AND RECOMMENDATIONS

[39] Section 13(1) allows a public body to refuse to disclose information that would reveal advice or recommendations developed by or for a public body. The purpose of s. 13(1) is to prevent the harm that would occur if a public body's deliberative process was exposed to public scrutiny.[27]

[40] The test under s. 13(1) is well-established, and I will apply it below.

Section 13(1) – would disclosure reveal advice or recommendations

[41] The first step in the s. 13 analysis is to determine whether disclosing the information at issue would reveal advice or recommendations developed by or for a public body.

[42] "Recommendations" involve "a suggested course of action that will ultimately be accepted or rejected by the person being advised."[28]

[43] "Advice" usually involves a communication, by an individual whose advice has been sought, to the recipient of the advice, as to which courses of action are preferred or desirable. However, the term "advice" has a broader meaning than the term "recommendations,"[29] and includes:

---

[26] Section 3(3)(f) applies to pp 71-73, 75-76, and 122-125 of the records.
[27] *Insurance Corporation of British Columbia v Automotive Retailers Association*, 2013 BCSC 2025 [*ICBC*] at para 52.
[28] *John Doe v Ontario (Finance),* 2014 SCC 36 [*John Doe*] at para 24.
[29] *John Doe ibid* at para 23.

- a communication as to which courses of action are preferred or desirable,[30] and
- an opinion that involves exercising judgment and skill to weigh the significance of matters of fact on which a public body must make a decision for future action.[31]

[44] Section 13(1) applies not only when disclosure of the information would directly reveal advice or recommendations, but also when it would allow accurate inferences to be drawn about advice or recommendations.[32]

Parties' submissions

[45] The Ministry describes the records containing the information it withheld under s. 13(1) as email communications between the CVAP Director and the CIO Employee. It states that disclosing this information would reveal advice and recommendations the CIO Employee provided to the Director about the privacy incident and the Ministry's notification obligations. In support of its position, the Ministry relies on affidavit evidence from the Director, who states that they received advice and recommendations from the CIO Employee regarding how to address the breach and respond to the applicant.[33]

[46] The applicant did not address s. 13(1) or respond to the Ministry's submissions.

Findings and analysis

[47] The Ministry withheld information from four email messages between the CVAP Director and CIO Employee under s. 13(1).[34] Having reviewed those emails, I find that the information the Ministry withheld under s. 13(1) is:

- the CVAP Director's suggestions about how the Ministry might address the privacy incident together with requests for the CIO employee's advice about those suggestions;[35]

[30] Order 01-15, 2001 CanLII 21569 at para 22.
[31] *College of Physicians of BC v. British Columbia (Information and Privacy Commissioner)*, 2002 BCCA 665 [*College*] at para 113.
[32] See for example *John Doe supra* note 28 at para 24; Order 02-38, 2002 CanLII 42472 (BCIPC); Order F10-15, 2010 BCIPC 24 (CanLII); and Order F21-15, 2021 BCIPC 19 (CanLII).
[33] Ministry's initial submissions, tab 2, affidavit of the CVAP Director at para 10.
[34] The information the Ministry withheld under s. 13(1) is found on pp 85, 89, 93, 100 and 115 of the records.
[35] The information at pp 85, 89, 93 are all duplicates of the same email from the CVAP Director to the CIO employee. The information at p 115 is found in a different email that is also from the Director to the investigator.

- the CIO Employee's description of the Ministry's decision about notifying the applicant; [36] and
- The CIO Employee's outline of the considerations relevant to the Ministry's decision about notifying the applicant.[37]

The CVAP Director's suggestions and requests for advice

[48] The responsive records include several emails between the CVAP Director and the CIO Employee. Having reviewed their communications, I find that they reveal a working relationship in which the CIO Employee advised the Director about how CVAP should address the privacy incident, and the two exchanged opinions on this topic. I also find that neither individual was the final decision maker with respect to responding to the information incident. In this regard, I note that in one of the records the Ministry disclosed, the CVAP Director makes clear that they cannot proceed without direction from their superior.[38] In this context, I accept that the Director's suggestions and their requests for advice about those suggestions to the CIO Employee are the Director's opinions about which courses of action the Director believes the Ministry should take in addressing the privacy incident.[39] Therefore, I find that disclosing this information would reveal advice within the meaning of s. 13(1).[40]

The CIO employee's description of the Ministry's decision

[49] I do not accept that s. 13(1) applies to the CIO Employee's description of the Ministry's decision about notifying the applicant. The description appears in an email the CIO Employee sent to the Director closing the CIO's file. It is clear on the face of the email that it was drafted after the Ministry made and implemented its decision about notifying the applicant of the breach.

[50] Section 13(1) is intended to protect a public body's deliberative process, not the outcome of those processes.[41] As such, information that communicates only the content of a finalized decision does not qualify as advice or recommendations under s. 13(1).[42] Consistent with the OIPC's past orders, I do not accept that s. 13(1) applies to the CIO employee's statement describing a decision that the Ministry had already made and implemented.[43]

---

[36] Records p 100.
[37] This information is also found on p 100 of the Records.
[38] Exchange on p 118 of the Records.
[39] Order 01-15, 2001 CanLII 21569 at para 22.
[40] Section 13(1) applies to the information found on pp 85, 89, 93, 100, and 115 of the records.
[41] Order F23-101, 2023 BCIPC 117 (CanLII) at paras 117 and 118.
[42] See for example Order F24-48, 2024 BCIPC 56 (CanLII) at para 38; Order F23-101, 2023 BCIPC 117 (CanLII) at paras 117, 118; Order F21-16, 2021 BCIPC 21 (CanLII) at para 22; Order F19-27, 2019 BCIPC 29 at para 32, Order F18-04, 2018 BCIPC 4 (CanLII), at para 83; Order F15-37, 2015 BCIPC 40 at para 22; and Order F15-33, 2015 BCIPC 36 at para 25.
[43] Section 13(1) does not apply to the first seven words the Ministry withheld from p 100.

The CIO employee's outline of the considerations relevant to the Ministry's decision

[51] However, I find that s. 13(1) applies to the CIO Employee's outline of the considerations relevant to the Ministry's decision about notifying the applicant. This information is also in the CIO Employee's file closure email to the Director. Given the CIO Employee's role in advising the Ministry about its notification obligations, I find that disclosing this information would reveal the advice the CIO Employee previously provided to the Ministry about what factors should be considered when deciding whether to notify the applicant.[44]

Section 13(2) – exceptions to refusing access under s. 13(1)

[52] The next step is to decide whether the information that I have found reveals advice or recommendations under s. 13(1), falls into any of the categories listed in s. 13(2). If s. 13(2) applies, that information cannot be withheld under s. 13(1).

[53] The Ministry asserts that none of the exceptions in s. 13(2) apply. The applicant does not address s. 13(2).

[54] Having examined the categories in s. 13(2), I find that none apply.

Section 13(3) – information in existence for 10 or more years

[55] The third step is to consider whether the information has been in existence for more than 10 years under s. 13(3). Information that has been in existence for more than 10 years cannot be withheld under s. 13(1).

[56] The five email messages at issue and the document titled "incident summary" were prepared in response to the privacy incident which took place in 2022. They have not been in existence for more than 10 years. I find that s. 13(3) does not apply.

Conclusion – s. 13(1)

[57] In conclusion, I find that s. 13(1) authorizes the Ministry to refuse to disclose all the information it withheld under s. 13(1),[45] except the information that reveals its decision about notifying the applicant of the breach.[46]

[44] Section 13(1) applies to the balance of the information the Ministry withheld from p 100.
[45] Section 13(1) applies to the information the Ministry withheld from pp 85, 89, 93, and 115 and part of p 100 of the records.
[46] Section 13(1) does not apply to some of the information found on p 100 of the records.

Discretion under s. 13(1)

[58] Section 13 is a discretionary exception to access under FIPPA. In past orders, the OIPC has made clear that when considering discretionary exceptions to disclosure, a public body must "exercise that discretion in deciding whether to refuse access to information, and upon proper considerations,"[47] and must "establish that they have considered, in all the circumstances, whether information should be released even though it is technically covered by the discretionary exception."[48]

[59] If the head of the public body has failed to exercise their discretion, the Commissioner can require the head to do so. The Commissioner can also order the head of the public body to reconsider the exercise of discretion where the decision was made in bad faith or for an improper purpose, the decision took into account irrelevant considerations, or the decision failed to take into account relevant considerations.[49]

[60] The applicant submits that the Ministry has not reasonably exercised its discretion to withhold records under s. 13(1) of *FIPPA*. In her view, CVAP's notification letter was inadequate given the circumstances of the privacy incident and its impact on her.

[61] The Ministry responds that the applicant provided no reasons to support her position that it failed to appropriately exercise its discretion to withhold information under s. 13(1).

[62] The onus is on the Ministry to establish that it properly exercised its discretion under s. 13(1) – that is, that it considered, in all the circumstances, whether the information that it withheld under s. 13(1) should be released even though it may be technically covered by s. 13(1). In this case, the applicant put the question of the Ministry's exercise of discretion under s. 13(1) squarely in issue. The Ministry's assertion that it appropriately exercised its discretion neither identifies what factors it considered in exercising its discretion to deny access under s. 13(1) nor offers any evidence that it considered all relevant considerations and did not consider any irrelevant considerations.

---

[47] Order 02-50, 2002 CanLII 42486 (BC IPC) at para 144 and the cases citing it, for recent examples see Order F24-73, 2024 BCIPC 83 (CanLII) at para 187 and Order F24-88, 2024 BCIPC 100 (CanLII) at para 97.
[48] Order No 325-1999, [1999] BCIPCD No 38 at p 4 and the cases citing it. For recent examples see Order F24-73, 2024 BCIPC 83 (CanLII) at para 187 and Order F24-88, 2024 BCIPC 100 (CanLII) at para 97.
[49] Order F23-51, 2023 BCIPC 59 at para 142, citing *John Doe, supra* note 28 at para 52 and Order 02-38, 2002 CanLII 42472 (BC IPC) at para 147.

[63] As noted above, the Commissioner may return the matter to a public body for reconsideration where there is no evidence that the public body took into account relevant considerations in exercising its discretion under s. 13(1). In the absence of any such evidence, I find it is appropriate to order the head of the Ministry to reconsider their decision to refuse to disclose the information that I found is covered by s. 13(1).[50] As part of that reconsideration, I recommend the Ministry consider the circumstances identified in the OIPC's past orders which may be relevant in the circumstances of this access request.[51]

SECTION 22 – UNREASONABLE INVASION OF THIRD-PARTY PERSONAL PRIVACY

[64] Section 22(1) of FIPPA requires a public body to refuse to disclose personal information if the disclosure would be an unreasonable invasion of a third party's personal privacy.

Personal information

[65] As s. 22(1) only applies to personal information, the first step in the s. 22(1) analysis is to determine whether the information in dispute is personal information within the meaning of FIPPA.

[66] Personal information is defined in FIPPA as "recorded information about an identifiable individual other than contact information." Information is "about an identifiable individual" when it is "reasonably capable of identifying an individual, either alone or when combined with other available sources of information."[52]

[67] "Contact information" is defined in FIPPA as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual."[53]

[68] The Ministry applied s. 22(1) to information found in 13 pages of records which relate to the privacy incident.[54] The Ministry partially severed two of those pages and withheld the remaining 11 pages in their entirety. The information in dispute is found in a declaration signed by Employee 2 and email communications amongst Ministry employees (including Employees 1 and 2) in relation to the privacy incident. The CIO employee is copied on some of these emails. Having reviewed the withheld information, I find that it is:

---

[50] I found s. 13(1) applies to the information the Ministry withheld from pp 85, 89, 93, 115, and part of p 100 of the records.
[51] See for example Order 02-38, 2002 CanLII 42472 at para 149. and F08-03, 2008 CanLII 57363 (BC IPC) at para 38.
[52] Order F19-13, 2019 BCIPC 15 at para 16, citing Order F18-11, 2018 BCIPC 14 at para 32.
[53] Schedule 1.
[54] The information the Ministry withheld under s. 22(1) is found on pp 98-99, 103-104, 112-113, 120, and 126-131 of the records.

A. names, email addresses, and telephone numbers of Employees 1 and 2, other CVAP employees, and the CIO Employee;
B. information about Employee 1 and 2's involvement in the privacy incident;
C. CVAP employees' (including Employee 1 and 2's) questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident;
D. a CVAP employee's work location; and
E. email subject lines, sent dates, confidentiality disclaimers, salutations and pleasantries, office telephone numbers, and office addresses.

[69] For the reasons set out below, I find that some of the information is personal information within the meaning of FIPPA.

[70] **Group A:** A name is the most direct means of identifying an individual.[55] The email addresses include the individuals' names. Telephone numbers are for specific individuals, and in my view, given the small number of individuals involved, could be used to determine individuals' identities. Therefore, I find that this information is recorded information about identifiable individuals.

[71] Some of the names, email addresses, and telephone numbers are found in the sender and recipient fields and email signature blocks of work-related email messages. Past orders have routinely held that this kind of information is contact information because its purpose is to enable an individual to be contacted at their place of business.[56] However, ultimately, whether information is "contact information" depends on the context in which it appears.[57]

[72] The information of Employees 1 and 2 arises in the context of the privacy incident. As a result, disclosing their information would reveal not only how to contact them, but also the fact that they were involved in the privacy incident. In this context, I find that their names, telephone numbers, and email addresses are not contact information, and thus are personal information.

[73] I come to the opposite conclusion about the names and email addresses of the other CVAP employees and the CIO employee where it is found in email signature blocks or sender or recipient fields of emails. The information about these individuals is found in emails in which these individuals provided received questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident, otherwise put, in which they went about their regular job duties. In this context, I see no reason to depart from the OIPC's typical approach. I find that the names, telephone numbers, and email addresses of the

[55] See for example Order F21-47, 2021 BCIPC 55 (CanLII) at para 13.
[56] See for example Order F21-40, 2021 BCIPC 48 (CanLII) at para 50, Order F20-37, 2020 BCIPC 43 (CanLII) at para 81, and Order F24-48, 2024 BCIPC 56 (CanLII) at paras 72 and 73.
[57] See Order F20-13, 2020 BCIPC 15 (CanLII) at para 42 and Order F24-81, 2024 BCIPC 93 (CanLII) at para 60.

other CVAP Employees and CIO Employee are contact information and therefore excluded from the definition of personal information.

[74] **Groups B – D:** The information about Employee 1 and 2's involvement in the privacy incident; CVAP employees' questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident; and a CVAP employee's work location arise in the context of a specific incident involving a limited number of individuals and are found in records that refer to these individuals by name. I find that anyone familiar with the circumstances of the privacy incident could easily connect this information to the individuals referred to and named. I find that this information is about identifiable individuals. As it is clearly not contact information, I find that it is personal information.

[75] **Group E:** However, I am not persuaded that the balance of the information is personal information – that is the email subject lines, sent dates, confidentiality disclaimers, salutations, office telephone numbers, office addresses, and titles of documents. I find that this information is too general to be about any specific individual.

[76] **Conclusion:** In summary, I find that only the following information in dispute is personal information within the meaning of FIPPA:

a) Employee 1 and 2's names, email addresses, and telephone numbers, and the names of other CVAP employees where their names are found in the body of email messages;
- information about Employee 1 and 2's involvement in the privacy incident;
- CVAP employees' names;
- CVAP employees' (including Employee 1 and 2's) questions, concerns, opinions, and instructions about the Ministry's response to the incident; and
- a CVAP employee's work location.

Section 22(4) – Circumstances where disclosure is not an unreasonable invasion of a third party's personal privacy

[77] The second step in the s. 22 analysis is to consider whether s. 22(4) applies to any of the information that I have found is personal information. Section 22(4) lists circumstances where disclosure of personal information is not an unreasonable invasion of a third party's personal privacy. If information falls into one of the circumstances enumerated in s. 22(4), the public body is not required to withhold it under s. 22(1).

[78] The parties raised ss. 22(4)(c) and (e).

Enactment authorizes the disclosure – s. 22(4)(c)

[79] Section 22(4)(c) provides that a disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if an enactment of British Columbia or Canada authorizes the disclosure.

[80] The applicant submits that s. 22(4)(c) is satisfied because she intends to obtain the information in dispute under the *Supreme Court Civil Rules* (the Rules)[58] through her Civil Claim, and then to rely on the information at the trial of her Civil Claim, thus making the information publicly available under the Rules.

[81] The Ministry submits that to the extent the applicant is seeking disclosure of the information for the purposes of pursuing the Civil Claim, she should be doing so pursuant to the Rules, and not under FIPPA.

[82] The Employees submit that to interpret s. 22(4)(c) in the manner proposed by the applicant would provide any access applicant with a general right of access to all documents that may be producible in litigation, thus enabling access applicants to make those documents public, and defeating the purpose of the implied undertaking of confidentiality in the Rules.

[83] Section 22(4)(c) stipulates that a disclosure of personal information is not an unreasonable invasion of privacy where (1) an enactment (2) authorizes disclosure of that personal information. While I accept that the enactment requirement is met, I do not accept that the "authorizes the disclosure" requirement is.

[84] The Rules are a regulation made under the *Court Rules Act*.[59] While the term "enactment" is not defined in FIPPA or its regulation, the *Interpretation Act,* defines an "enactment" as "an Act or a regulation or a portion of an Act or regulation.[60] I accept the definition in the *Interpretation Act,* and based on it, I find that the Rules are an enactment.

[85] To satisfy the second requirement, the enactment at issue, in this case the Rules, must authorize disclosure of the information that is in dispute. There are two problems here. First, the Rules do not authorize disclosure of any information. Rather, they create a process through which a party to a specific court proceeding may seek production of documents that could be used to prove or disprove a material fact at trial.[61] Second, the Rules do not address the information at issue, and I decline to adopt the applicant's speculative arguments

[58] BC Reg 168/2009.
[59] RSBC 1996, c 80.
[60] RSBC 1996, c 238, s. 1. For a similar approach, to the definition of the term enactment, see for example Order F24-54, 2024 BCIPC 64 (CanLII) at para 23 and Order F22-50, 2022 BCIPC 57 at paras 43-44.
[61] Rule 7.

about what might happen during the litigation of the Civil Claim into the interpretation of s. 22(4)(c).

[86] Ultimately, neither the Rules nor the applicant's position conform with the second requirement of s. 22(4)(c) – that is the Rules do not authorize disclosure of the information that is in dispute. I find that s. 22(4)(c) does not apply.

Third party's position, functions, or remuneration – s. 22(4)(e)

[87] Section 22(4)(e) provides that disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if the information is about the third party's position, functions, or remuneration as an officer, employee, or member of a public body.

[88] Section 22(4)(e) applies to "objective, factual statements about what the third party did or said in the normal course of discharging [their] job duties, but not qualitative assessments or evaluations of such actions."[62] When assessing whether s. 22(4)(e) applies, the key question is, considered in its full context, what does the information reveal about the affected individual?[63]

[89] The Ministry argues that s. 22(4)(e) does not apply to the information in dispute because the information is not objective, factual statements about what a third party did or said in the normal course of discharging their job duties but rather identifies the individuals who accessed the applicant's personal information without a business purpose for doing so, which is not part of their ordinary work duties. The applicant and Employees do not address s. 22(4)(e).

[90] Some of the personal information at issue is about Employees 1 and 2. The information about Employees 1 and 2 relates to their conduct in relation to the privacy incident. There is no dispute that this conduct fell outside of the scope of the normal course of their job duties. Therefore, I find that s. 22(4)(e) does not apply to any of the personal information of the Employees.

[91] The Ministry also withheld the names, questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident of other CVAP employees. The information is found in emails in which these employees answered questions and gave instructions related to the Ministry's response to the privacy incident. I find these actions relate to the regular job functions of these employees, and that disclosing this information would reveal the kind of objective, factual statements about what these individuals did or said in the normal course of discharging their job duties to which s. 22(4)(e) typically

[62] Order 01-53, 2001 CanLII 21697 (BC IPC) at para 40 and the cases citing it.
[63] See for example Order F23-28, 2023 BCIPC 32 at para 42; Order F21-08, 2021 BCIPC 12 (CanLII) at paras 126-129; Order F10-21, 2010 BCIPC 32 (CanLII) at para 24; Order F08-04, 2008 CanLII 13322 (BC IPC) at para 27; Order 00-53, 2000 CanLII 14418 (BC IPC) at page 7; and Order 01-53, 2001 CanLII 21607 (BC IPC) at para 40.

applies. Accordingly, I conclude that s. 22(4)(e) applies to all the personal information that remains at issue that is not about Employees 1 and 2.[64]

[92] Having considered the remaining subsections in s. 22(4), I find that no others apply.

Section 22(3) – Disclosure presumed to be an unreasonable invasion of third-party personal privacy

[93] Section 22(3) lists circumstances where disclosure is presumed to be an unreasonable invasion of a third party's personal privacy. The third step in the s. 22 analysis is to consider whether the presumptions listed in s. 22(3) apply to any of the personal information that is not excluded under s. 22(4). Given my finding above, the information that remains at issue is Employee 1 and 2's names, email addresses, telephone numbers, information about their involvement in the privacy incident, their questions and concerns about the Ministry's response to the privacy incident, and some other CVAP Employees' questions, concerns, opinions, and instructions that are also about Employees 1 and 2.

[94] The parties made arguments about ss. 22(3)(b) and (d). I will consider these presumptions below.

Investigation into a possible violation of law – s. 22(3)(b)

[95] Section 22(3)(b) provides that a disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if 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.

[96] The applicant submits that s. 22(3)(b) applies but weighs in favour of disclosure. The Ministry and the Employees submit that s. 22(3)(b) does apply.

[97] Section 22(3)(b) describes a presumption against disclosure. There is no circumstance where a finding that s. 22(3)(b) applies could weigh in favour of disclosure (as the applicant submits). Although for different reasons, all the parties agree that s. 22(3)(b) does not operate to create a presumption <u>against</u> disclosure of the information in dispute. For the reasons below, I agree.

---

[64] I note that the some of the information at issue is at the same time about Employees 1 and 2 and about other CVAP employees. Where the information is also about Employees 1 and 2, it is not excluded under s. 22(4)(e) because of what it would reveal about Employees 1 and 2. However, in considering this information further, I will not consider the privacy interests of the other CVAP employees because, as discussed in para 91, disclosure of the information at issue would not be an unreasonable invasion of their privacy.

[98] For s. 22(3)(b) to apply, the information at issue must be (1) compiled and identifiable as part of an investigation, and (2) that investigation must be into a possible violation of law.

[99] With respect to the first requirement, past orders have held that compiling information involves some exercise of judgment, knowledge, or skill on behalf of the public body.[65] While little has been written about the "identifiable" requirement, in my view, it requires, at a minimum, that the information be somehow recognizable as connected to an investigation. Regarding the second requirement, past orders have defined the term "law" as including a legislative provision, the violation of which could result in a penalty or sanction.[66] I adopt the above definitions for the purpose of my analysis.

[100] The information at issue is found in Employee 2's declaration and in CVAP employees' emails about the privacy incident and the Ministry's response to it. While some of the information appears to relate to the Ministry's efforts to determine what happened and how the Ministry should respond to the privacy incident, on the evidence before me, I am unable to find that these efforts relate in any way to a violation of any law. In making this finding, I wish to be clear that while some of the records and information at issue under ss. 3 and 13 related to the applicant's OIPC Privacy Complaint, the information at issue under s. 22(1) does not. Rather, the records containing the information at issue under s. 22(1) predate the OIPC Privacy Complaint and appear to have been created for the Ministry's internal purposes, to decide how it should respond to the privacy incident. There is no evidence before me (and no party suggests) that any of the requirements in s. 22(3)(b) are met. Accordingly, I find that s. 22(3)(b) does not apply to the information in dispute.

Employment, occupational or educational history – s. 22(3)(d)

[101] Section 22(3)(d) creates a presumption against disclosure where personal information relates to the employment, occupational, or educational history of a third party.

[102] Pointing to past orders in which the OIPC has held that "employment history" includes descriptive information about a third party's workplace behavior or actions in the context of a workplace complaint investigation or disciplinary matter,[67] the Ministry submits that the circumstances before me, while not about a disciplinary issue, are analogous to these past cases because the privacy incident triggered an OIPC investigation and civil litigation against the Ministry.

---

[65] Order F19-02, 2019 BCIPC (CanLII) at para 39; Order F23-78, 2023 BCIPC 90556 (CanLII) at para 95; and Order F24-10, 2024 BCIPC 14 (CanLII) at para 67.
[66] See for example Order 01-12, 2001 BCIPC 21566 (CanLII) at para 17; Order F22-31, 2022 BCIPC 34 (CanLII) at para 53; and Order F24-10, 2024 BCIPC 14 (CanLII) at para 73.
[67] See Order 01-53, 2001 CanLII 21607 (BC IPC) at paras 32-38; and Order F21-08, 2021 BCIPC 12 (CanLII) at para 137.

[103] The Employees also submit that s. 22(3)(d) applies, emphasizing that the information at issue relates to an investigation into a workplace matter involving the conduct of Employees 1 and 2 in which they were the subject of, rather than mere participants in the investigation.

[104] The applicant does not address s. 22(3)(d).

[105] Past orders have consistently held that "employment history" includes qualitative information about a third party's workplace behaviour,[68] particularly as it relates to individuals who are the subject of workplace complaints.[69]

[106] Employees 1 and 2 were involved in a privacy incident at work that resulted in a privacy complaint to the OIPC and civil litigation against the Ministry. All the information that remains in dispute is the personal information of Employees 1 and 2. It identifies Employees 1 and 2 and/or describes the conduct that resulted in the privacy incident. I find the information reveals qualitative details about Employee 1 and 2's workplace conduct, in a context where they were the actors in a serious workplace incident. For these reasons, I find that the information that remains in dispute is Employee 1 and 2's employment history, and that s. 22(3)(d) applies to all of it.

[107] Having considered the remaining subsections in s. 22(3), I find that no others apply.

Section 22(2) – All relevant circumstances

[108] The final step in the s. 22 analysis is to consider the impact of disclosing the personal information at issue in light of all relevant circumstances, including those listed in s. 22(2). It is under s. 22(2) that the s. 22(3) presumptions against disclosure – in this case s. 22(3)(d) – may be rebutted.

[109] The parties raised ss. 22(2)(a), (c), (e), (f), the applicant's ability to obtain the information through an alternative avenue, and the applicant's motivation for seeking access. I will consider each in turn.

Scrutiny of a public body – s. 22(2)(a)

[110] Section 22(2)(a) requires a public body to consider whether "the disclosure is desirable for the purpose of subjecting the activities of … a public body to public scrutiny." Section 22(2)(a) recognizes that where disclosure of the information in dispute would foster accountability of a public body, this may

[68] See for example Order 01-53 2001 CanLII 21607 (BCIPC) at paras 32-33; Order F16-28, 2016 BCIPC 30 (CanLII) at para 94; and Order F24-81, 2024 BCIPC 93 (CanLII) at para 73.
[69] See for example Order 01-53, 2001 CanLII 21607 (BCIPC) at paras 32 and 41; Order F20-13, 2020 BCIPC 15 (CanLII) at para 55; and Order F24-81, 2024 BCIPC 93 (CanLII) at para 73.

provide a foundation for finding that disclosure would not constitute an unreasonable invasion of a third party's personal privacy.[70] However, for s. 22(2)(a) to apply, the disclosure of the specific information at issue must be desirable for subjecting the public body's activities to public scrutiny as opposed to subjecting an individual third party's activities to public scrutiny.[71]

[111] The applicant submits s. 22(2)(a) applies because the information in dispute is desirable for the purpose of subjecting the activities of the Ministry to public scrutiny regarding the lack of security measures it has in place to protect the privacy of individuals who apply to CVAP for benefits and for the manner in which it deals with privacy incidents and satisfies its notification obligations. In addition, the applicant submits that s. 22(2)(a) applies to Employee 2's declaration because Employee 2 later stated it contained inaccurate information.[72] The applicant submits that disclosing the declaration would reveal the false evidence the Ministry submitted during the investigation into the OIPC Privacy Complaint.

[112] The Ministry submits that s. 22(2)(a) does not apply because the information at issue has no broad or public significance and disclosing it would not benefit the public to an extent that warrants the resulting invasion of personal privacy.

[113] The Employees submit that s. 22(2)(a) does not apply because the information at issue is their personal information and disclosing it would submit them, rather than the Ministry to public scrutiny.

[114] The key question here is whether disclosing the information that remains in dispute would serve the purpose of subjecting the activities of the Ministry (rather than just Employees 1 and 2) to public scrutiny.

[115] I can see no connection between Employee 1 and 2's names, email addresses, and telephone numbers and the activities of the Ministry. Rather, in my view, disclosing this kind of information would only serve to subject Employees 1 and 2 to public scrutiny. I find that s. 22(2)(a) does not apply to this information.

[116] The balance of the information in dispute is information about Employee 1 and 2's involvement in the privacy incident, and CVAP employees' (including Employee 1 and 2's) questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident. While this information is the personal information of Employees 1 and 2, it also offers insight into what happened

[70] Order F05-18, 2005 CanLII 24734 (BC IPC) at para 49.
[71] Order F16-14, 2016 BCIPC 16 (CanLII) at para 40 and Order F24-48, 2024 BCIPC 56 (CanLII) at para 105.
[72] This statement is found in a letter signed by Employee 2 that the appropriate persons submitted with their submission in this inquiry.

regarding the privacy incident and how the Ministry responded. In my view, revealing this information would foster accountability of the Ministry by subjecting the activities of one of its programs to public scrutiny.

[117] Because of its role in providing compensation to victims of crime through CVAP, the Ministry collects and retains sensitive personal information from vulnerable individuals. The OIPC Investigator has already substantiated the applicant's OIPC Privacy Complaint.[73] In addition, the Ministry did not notify the applicant of the privacy incident until three months after it occurred.[74] In these circumstances, it is my view that the interest in subjecting the Ministry's activities to public scrutiny is an important one.

[118] I find that s. 22(2)(a) is a factor that favours disclosure of the information about Employee 1 and 2's involvement in the privacy incident, and CVAP employees' (including Employee 1 and 2's) questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident. [75]

Fair determination of the applicant's rights – s. 22(2)(c)

[119] Section 22(2)(c) requires a public body to consider whether the personal information is relevant to a fair determination of the applicant's rights.

[120] Past orders establish a four-part test, each step of which must be met in order for s. 22(2)(c) to apply:

> 1. The right in question must be a legal right drawn from the common law or a statute, as opposed to a non-legal right based only on moral or ethical grounds;
>
> 2. The right must be related to a proceeding which is either underway or is contemplated, not a proceeding that has already been completed;
>
> 3. The personal information sought by the applicant must have some bearing on, or significance for, determination of the right in question; and
>
> 4. The personal information must be necessary in order to prepare for the proceeding or to ensure a fair hearing.[76]

[73] OIPC Investigator's letter dated February 22, 2023, applicant's initial submission, tab 2, affidavit of the applicant, exhibit O.
[74] See paras 13 and 15 above.
[75] As this finding applies to the information in Employee 2's declaration, I need not consider the applicant's arguments about the impact of disclosing the declaration independently.
[76] Order 01-07, 2001 CanLII 21561 (BCIPC) at para 31; Order F15-11, 2015 BCIPC 11 at para 24; and Order F24-09, 2024 BCIPC 12 (CanLII) at para 48.

[121] The applicant asserts that the information in dispute is relevant to a fair determination of her legal rights in the Civil Claim.[77] Specifically, the applicant states that the Ministry's response to the Civil Claim is late and that the Ministry has not provided any disclosure in the Civil Claim, and that as a result, she requires the information in dispute to determine how best to proceed with the Civil Claim. The applicant also states that she requires the names of Employees 1 and 2 to be able to serve them with the Notice of Claim in accordance with Rule 3 of the Rules so that she does not lose the right to proceed against them in the Civil Claim.

[122] The Ministry characterizes the Civil Claim as concerning whether the Ministry breached the standard of care in safeguarding the applicant's personal information. The Ministry submits that this issue can be determined without the identity of the Employees. Thus, the Ministry argues that the applicant does not require the information at issue to prepare for or ensure a fair hearing of the Civil Claim.

[123] The Employees submit that s. 22(2)(c) does not apply because the information at issue is available through the Civil Claim. They also argue in the alternative that the fact that the information is available through the Civil Claim, which is already underway, and which would offer greater privacy protections is nevertheless a relevant consideration under s. 22.

[124] The applicant filed the Civil Claim against the Minister, the Director, and five unnamed CVAP employees. In the Notice of Claim, the applicant alleges, among other things, that CVAP employees violated FIPPA and the *Privacy Act* by snooping on her personal information, and that the Minister and Director were vicariously liable for the employees' actions. The applicant also alleges that the Minister and the Director breached the standard of care owed to her as a client of CVAP by failing to take steps to mitigate the risk of unauthorized access to client files, and by failing to promptly notify her of the breach.[78] There is no dispute that the Civil Claim is ongoing.

[125] Parts one and two of the s. 22(2)(c) test require that the right in question be a legal right that relates to a proceeding that is underway or contemplated. Relying on the facts set out above, I have no difficulty finding that the first two steps of the test are met in respect of the Civil Claim.

---

[77] While the applicant also made arguments about family law proceedings, her rights under FIPPA and the *Privacy Act* RSBC 1996, c 373, and her intention to request a reconsideration of the disposition of the OIPC Privacy Complaint, I have not addressed these arguments here given my findings that s. 22(2)(c) favours disclosure given the ongoing Civil Claim.

[78] Notice of Civil Claim at paras 24-44, applicant's initial submission, Tab 2, affidavit of the applicant, exhibit A.

[126] Part three requires that the personal information sought by the applicant have some bearing on, or significance for, a determination of the legal right in question. That is, the applicant must prove there is a "demonstrable nexus" or "connection" between the withheld information and the legal right. In other words, the personal information at issue must have some significance for the determination or implementation of the legal right.[79]

[127] The applicant states that one purpose for which she seeks the information is to identify and serve the defendant employees with the Notice of Claim. In my view, the applicant's ability to know the names of and to contact the persons she alleges breached FIPPA and the *Privacy Act* goes to the core of her ability to pursue her legal action and potentially obtain relief against them. Therefore, I find the names, telephone numbers, and email addresses of Employees 1 and 2 has significance for the implementation and determination of the applicant's legal rights.

[128] I also find that the information about Employee 1 and 2's involvement in the privacy incident and CVAP Employees' questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident satisfies the third part of the test. This information reveals information about what happened and how the Ministry responded to the privacy incident. The applicant alleges that by failing to promptly notify her of the breach, the Director and the Ministry breached the standard of care owed to her as a client of CVAP. The applicant will require evidence about the privacy incident and the Ministry's response to it to assess or prove this allegation. Therefore, in my view, there is a clear and direct connection between this information and the determination of the applicant's claims against the Ministry and the Director in the Civil Claim.

[129] Part 4 of the test requires that the information be necessary in order to prepare for the proceeding or to ensure a fair hearing. Most past orders hold that to satisfy this part of the s. 22(2)(c) test, the applicant need only prove that the personal information itself is necessary to prepare for the proceeding or to ensure a fair hearing, not that the FIPPA process is the only way they can access the information.[80] I agree with and adopt this approach – the fourth step of the test asks whether the information itself is necessary, not whether disclosure under FIPPA is necessary to obtain a copy of the disputed records.[81] Therefore, the relevant question is whether the information itself is necessary to prepare for the proceeding or to ensure a fair hearing – in this case, of the Civil Claim.

---

[79] See for example Order F24-17, 2024 BCIPC 23 (CanLII) at para 153; Order F24-48, 2024 BCIPC 56 (CanLII) at paras 122-124, Order F23-65, 2023 BCIPC 75 (CanLII) at para 145, Order F16-36, 2016 BCIPC 40 (CanLII) at paras 52 and 62 and Order F16-36, 2016 BCIPC 40 (CanLII).
[80] See for example Order F16-36, 2016 BCIPC 40 (CanLII) at para 56,
[81] See Order F24-57, F24-49, 2024 BCIPC 57 at para 107; Order F23-13, 2023 BCIPC 15 (CanLII), at paras 151-154; and Order F16-36, 2016 BCIPC 40 (CanLII) at para 59 for similar reasoning.

[130] The applicant states that she requires the names of Employees 1 and 2 so that she can name them as defendants in the Civil Claim and serve them with the Notice of Claim as required by the *Rules.* While the Employees acknowledge that the applicant has not yet served them,[82] neither the Ministry nor the Employees address directly the applicant's position in this regard.

[131] I find that naming and serving all defendants to a civil proceeding is a necessary part of preparing for that proceeding. The applicant does not know the identity of the Employees or have access to a means of contacting them. I accept that knowing the names and how to contact the persons she wishes to name in and serve with the Notice of Claim is necessary for the applicant to prepare for the Civil Claim and to ensure a fair hearing of her allegations against those individuals. Accordingly, I accept that Employee 1 and 2's names, telephone numbers, and email addresses satisfy the fourth step of the test.

[132] I also accept that information about Employee 1 and 2's involvement in the privacy incident and CVAP Employees' questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident is necessary to ensure a fair hearing. This information sets out what happened to the applicant's information and how the Ministry responded. I find that it is directly relevant to proving or disproving the applicant's claims about whether the privacy incident constituted a breach of FIPPA and the *Privacy Act,* and whether the Minister and/or Director breached the standard of care owed to the applicant by failing to mitigate the risk of unauthorized access to client files and by failing to promptly notify her of the breach. Therefore, I find that this information also satisfies the fourth steps of the s. 22(2)(c) test.

[133] For the reasons discussed above, I find that s. 22(2)(c) weighs in favour of disclosure of all the information that remains in dispute.

Applicant's ability to obtain the information through the Civil Claim

[134] I now turn to the Employees' alternative argument that the fact that the information will be available through the Civil Claim is a relevant consideration under s. 22(1). I do not accept this proposition. First, this submission is hypothetical. The applicant has not yet obtained disclosure under the Rules, and it is not clear that she will. Second, I am not aware of any OIPC orders that have considered this to be a relevant circumstance, and the Employees did not identify any. Finally, to accept this argument would, in my view, undermine the OIPC's preferred approach to the interpretation of s. 22(2)(c). As discussed above, s. 22(2)(c) concerns the relevance of the information to a fair determination of the applicant's rights, not the applicant's ability to access that information through other means. To accept the Employee's alternative argument would be to adopt

[82] Appropriate parties' submission at para 39.

the interpretation of s. 22(3)(c) I have rejected under a different name. I decline to do so.

Unfair risk of financial or other harm and Unfair damage to reputation – ss. 22(2)(e) and (h)

[135] Section 22(2)(e) concerns whether disclosure of a third party's personal information will unfairly expose the third party to financial or other harm. Harm under s. 22(2)(e) can include mental harm, in the form of serious mental distress or anguish, but embarrassment, upset or having a negative reaction do not rise to the level of mental harm required under s. 22(2)(e).

[136] Section 22(2)(h) concerns whether the disclosure may unfairly damage the reputation of any person referred to in the records requested by the applicant. Two requirements must be met in order to engage s. 22(2)(h). First, the information must damage an individual's reputation. Second, that damage must be unfair.

[137] The Employees submit that both ss. 22(2)(e) and (h) favour withholding their personal information. In letters that accompanied their inquiry submissions, the Employees explained in detail how disclosing their information and thus connecting them to the privacy incident and the allegations in the Notice of Claim would harm their mental health, ability to function personally and professionally, and the well-being of their families. They also suggest that naming them publicly may "give space" for harassment against them and their loved ones. The Employees further assert that disclosing their names would harm their reputations and ability to perform their roles in CVAP because it may cause clients and other entities to question their trustworthiness. In support of these submissions, the Employees emphasize the value they place on their work, the importance of being seen as trustworthy given the nature of their work, and the fact that that allegations in the Notice of Claim are unproven.

[138] The Employees also submit that the harm would be unfair within the meaning of ss. 22(2)(e) and (h) because disclosure of their personal information would connect them to the very serious and unproven allegations found in the Notice of Claim. They also rely on Order No. 237-1998,[83] for the proposition that disclosing information that would allow an access applicant to name defendants in a lawsuit creates unfair harm. The Employees also assert that the harm would be unfair because some of the information in the declaration inaccurately suggests that Employee 2 read more of the applicant's application to CVAP than they did.

[83] 1998 CanLII 3539 (BC IPC).

[139] Furthermore, noting that the Civil Claim has already received media attention and scrutiny, the Employees submit that unlike the applicant, who has obtained a publication ban in the Civil Claim, if their identities are disclosed through this inquiry, they will have no control over how their identities are shared or with whom. They also submit that if they are ultimately made parties to the Civil Claim, that they intend to seek a publication ban, which will be moot if their identities are disclosed through this inquiry.

[140] The Ministry's submissions are limited to the harm aspect of s. 22(2)(h). The Ministry submits that the OIPC's past orders have consistently held that the harm caused by disclosing personal information is unfair where the information amounts to unproven allegations against the individual affected and that individual did not have an opportunity to rebut the allegations in the context of an investigative process.[84] Relying on these cases, the Ministry submits that disclosure of the Employees' names would cause harm to the Employees' reputations because the allegations against them in the Notice of Claim are not proven.

[141] The applicant's extensive submissions on these issues can be distilled down to a few sentences: "If an individual has chosen to commit a violation of the law, then disclosure of that fact – along with any impact it may have on the wrongdoer, or their reputation – is not unfair. Individuals should be held accountable for unlawful acts they choose to engage in, particularly when they are misusing power and resources that have been conferred upon them by a public body."[85] In support of this position, the applicant also cites several court and tribunal decisions as well as decisions of information and privacy commissioners from other provinces in which decision makers declined to withhold the identities of individuals against whom allegations of wrongdoing were made.

[142] For either s. 22(4)(e) or s. 22(4)(h) to apply, the harm or reputational damage must be unfair. As the issue of unfairness was the focus of the parties' submissions, I will deal with it first. Only if I decide that there is unfairness, will I go on to determine whether the Employees (or either of them) will be exposed to financial or other harm, or whether disclosure may damage their reputations within the meaning of s. 22(2)(e) and/or (h).

[143] Both the Ministry and the Employees point to the unproven nature of the allegations in the Notice of Claim as evidence of unfairness. I accept that the Notice of Claim, by its nature, contains unproven allegations. Given the applicant's intention to use Employee 1 and 2's names to identify and serve them with the Notice of Claim, I also accept that disclosing the information in dispute

[84] In support of this position, the Ministry cites Order F21-28, 2021 BCIPC 36 at paras 124-126; Order F20-37, 2020 BCIPC 43 at paras 131-132; Order F17-01, 2017 BCIPC 1 at para 61; Order F16-50, 2016 BCIPC 55 at paras 52-54.
[85] Applicant's initial submission at para 52.

will connect the Employees to those allegations. However, I do not accept that the unfairness requirement in either s. 22(2)(e) or (h) is met.

[144] To start, pleadings in civil claims are, by their nature, unproven allegations. Canada's judicial system operates on the basis that these unproven allegations are tested through proceedings in which all parties are able to lead evidence to prove or disprove those allegations. The Employees will have the opportunity to respond to any allegations with which they disagree. In my view, there is nothing inherently unfair about the exposure to harm or reputational damage that sometimes may result when parties to court proceedings are named in relation to unproven allegations against them. There is a general understanding that those claims have yet to be proven.

[145] The Employees also argue that unfairness arises because one of the statements in Employee 2's declaration is untrue and inaccurately suggests that Employee 2 read more of the applicant's file than they actually did. I do not accept that this submission engages s. 22(2)(e) or (h). It concerns a single piece of information. I am unable to see how the difference between improperly viewing part versus all, of the applicant's file could have any actual impact on how the disclosure affects the Employees, and the Employees have not explained. Furthermore, in terms of fairness, I note that it is Employee 2 who signed the declaration that they now allege is untrue.

[146] I turn now to Order No. 237-1998 which the Employees interpret to mean that it would be unfair to disclose information that would allow an access applicant to sue a third party. I do not read Order No. 237-1998 as broadly as the Employees suggest. The key passage in the order reads "*Given the history of the litigation*, I conclude that disclosure of the personal information may expose the third parties unfairly to financial harm."[86] The litigation history described in the order is one in which the access applicant lost at trial, lost again before the court of appeal, was denied leave to appeal by the Supreme Court of Canada, and then sought new evidence about a third party in order to renew his challenge of the trial court's decision and threatened to sue that third party if they did not consent to disclosure of their personal information.

[147] The facts of the applicant's Civil Claim bear no resemblance to the litigation history that informed the decision in Order No. 237-1998. In the normal course, a plaintiff to a civil claim knows the names of the defendants and can proceed against them. This system is not inherently unfair. In this case, the Employees have not explained how the circumstances or history of the Civil Claim are such that any exposure to harm or reputational damage they may experience as a result of the disclosure of information that will allow the applicant to proceed against them would be unfair.

[86] *Ibid* at p 5, my emphasis.

[148] I am similarly not persuaded by the Employees' submission about the mootness of a publication ban. A publication ban is not about withholding the identity of the defendants from another party to a court proceeding. It is about the publication of their names. Regardless of my decision in this inquiry, there is nothing to stop the Employees from seeking a publication ban from the Court in the Civil Claim. I note that the applicant did so in the Civil Claim despite the fact that all other parties know her name.

[149] Ultimately, the information at issue is facts about who did what in respect of the privacy incident and the Ministry's response to it. While disclosing information about the Employees will allow them to be connected to the allegations in the Notice of Claim and any media attention the case has received, there is nothing inherently unfair about any of this, and neither the Ministry nor the Employees have provided evidence that persuades me that any harm or reputational damage the Employees may experience as a result of disclosing their names or information about their involvement in the privacy incident, and thus allowing the Civil Claim to proceed, would be unfair.

[150] While I have considerable sympathy for the Employees and any distress that they may feel, I am not persuaded that any exposure to financial or other harm or potential reputational damage they may suffer as a result of the disclosure of their personal information would be unfair. For these reasons, I do not accept that s. 22(4)(e) or (h) apply to the information in dispute.

Applicant's motive

[151] An access applicant's motivation or purpose for wanting the personal information at issue may be a relevant circumstance that weighs in favour or against disclosure.

[152] The Ministry submits that the applicant's motivation weighs against disclosure of the information at issue because the applicant's motive for seeking the names of Employees 1 and 2 relates to the Civil Claim, and as the applicant knows and has referred to the name of Employee 2 in the Civil Claim,[87] it is not clear how the information in dispute will be of use in the Civil Claim.

[153] While the applicant does not address this argument directly, her submissions and affidavit offer insight into her motives.

[154] The applicant states that the Ministry never informed her who committed the privacy incident, what happened, why it concluded that her personal information had not been disclosed to anyone outside of CVAP, or what steps it took to investigate whether the information was, as she suspects, disclosed to the individual who committed the crimes against her (the accused). According to

[87] Ministry initial submission at para 83.

the applicant, because the Ministry refused to provide this information, she is seeking access to be able to assess and mitigate the safety risks she faces as a result of the privacy incident. In this regard, the applicant explains that in the days following the incident, the accused began behaving in a threatening manner toward her and that he had previously threatened to kill her if she reported his actions to the police. For this reason, the applicant states, it is particularly important to her to know whether the accused's family member was the individual who improperly accessed her file.

[155] The applicant also explains that she is seeking access to the information at issue to have sufficient information to manage the serious privacy concerns relating to ongoing communications with CVAP. The applicant explains that since learning of the privacy incident, she no longer feels safe communicating with anyone at CVAP, adding that because she does not know the identity of Employees 1 and 2, she cannot prevent them from being involved in her file.

[156] Finally, as discussed in relation to s. 22(2)(h), the applicant acknowledges that another purpose for which she seeks access to the personal information at issue relates to the Civil Claim.

[157] Having reviewed CVAP's privacy incident notification letter, I find that the applicant's submission accurately describes the information the Ministry did not provide her about the privacy incident. Therefore, I accept that the applicant has unanswered questions about the privacy incident and the identities of those involved. While the Ministry is correct that the applicant refers to an individual by name in the Civil Claim, it is clear from the fact that the applicant did not name Employee 2 in the Notice of Claim that the applicant suspects but does not know the identity of Employee 2, and neither the Ministry nor the Employees have confirmed that this individual was in fact involved in the privacy breach. In addition, there is more personal information at issue than just the name of any one individual. Consistent with past OIPC orders, I find that the fact that the applicant has unanswered questions about the privacy incident favours disclosure of the information that remains in dispute.[88]

[158] I also accept that the applicant has a legitimate interest in obtaining information so she can understand how best to mitigate the potential safety risks she faces as a result of the privacy incident. The applicant provided information about her safety interests by way of affidavit evidence. Neither the Ministry nor the Employees dispute this information. Considering the evidence before me, I find that the crimes were serious and that the circumstances suggest that the applicant may remain vulnerable to the individual who committed the crimes against her.[89] Thus, I find the applicant's evidence about her safety concerns to

[88] See for example Order F21-64, 2021 BCIPC 75 (CanLII) at para 111.
[89] My finding that the applicant may remain vulnerable is based on information in the applicant's affidavit found at tab 2 to the applicant's initial submission, information in the exhibits to that affidavit, and information in the responsive records including a decision by CVAP to award the

be plausible. Given the importance of these interests, I find that the applicant's motivation to use the disputed information to make decisions about her safety favours disclosure.

[159] I also accept that the applicant's motivation to use the information to manage her privacy concerns favours disclosure. The applicant has an ongoing relationship with CVAP. While I can see that the Ministry has taken steps to manage the applicant's privacy concerns following the privacy incident, it is also understandable that the applicant is not comfortable continuing to provide sensitive information to CVAP when she does not have enough information to know what happened and whether those involved in the privacy incident still have access to her file.

[160] Finally, for the reasons set out in respect of s. 22(2)(c) and above, I am not persuaded by the Ministry's argument that the applicant's interest in using the information in dispute to pursue the Civil Claim weighs against disclosure.

[161] Considering all the above together, I find that the applicant's motivation favours disclosure.

Section 22(1) – Conclusion

[162] I found that the names, email addresses, and telephone numbers of the CIO Employee and CVAP Employees other than Employees 1 and 2 as well as email subject lines, sent dates, confidentiality disclaimers, salutations and pleasantries, office telephone numbers, office addresses, and titles of documents were not personal information. Consequently, s. 22(1) does not apply to this information.

[163] I found that the balance of the information the Ministry withheld under s. 22(1) was personal information. That information is as follows:

b) names, email addresses, and telephone numbers of Employees 1 and 2, and the names of other CVAP employees where their names are found in the body of email messages;
c) information about Employee 1 and 2's involvement in the privacy incident;
d) CVAP employees' (including Employee 1 and 2) questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident; and
e) A CVAP employee's work location.

applicant financial benefits for expenses related to protection from the accused which is found at p 10 of the records.

[164] However, I found that s. 22(4)(e) applied to names, email addresses, telephone numbers, and the work location of CVAP employees other than Employees 1 and 2 and the CIO Employee. I found it also applied to the questions, concerns, opinions, and instructions about the Ministry's response to the privacy incident of CVAP employees other than Employees 1 and 2 to the extent that they did not also reveal information about Employees 1 and 2. Therefore, in accordance with s. 22(4)(e), I found disclosure of this information would not be an unreasonable invasion of personal privacy under s. 22(1).

[165] What remains is Employee 1 and 2's names, email addresses, and telephone numbers; information about their involvement in the privacy incident; CVAP employees' (including Employee 1 and 2) questions, concerns, instructions and opinions about the Ministry's response to the privacy incident (to the extent that they are about Employees 1 and 2). The question before me is whether it would be *unreasonable* invasion of Employee 1 and 2's personal privacy to disclose this information.

[166] I found that the s. 22(3)(d) presumption against disclosure of employment history information applied to all the information that remained in dispute. However, for the reasons below, I find that the presumption is rebutted.

[167] CVAP is a government organization that, because of its role, collects sensitive information about vulnerable persons to perform its function. In my view, this context makes the s. 22(2)(a) interest in subjecting its actions surrounding a privacy breach to public scrutiny an important one.

[168] In addition, as a result of the information the Ministry chose to exclude from its breach notification, the applicant has several unanswered questions about the privacy incident. As discussed above, the answers to these questions are directly relevant to the applicant's legal rights in the Civil Claim (s. 22(2)(c)).

[169] Furthermore, given my finding that the applicant may remain vulnerable to the accused, the serious nature of the crimes described in the applicant's file with CVAP, and the specific familial connection she described between the accused and the CVAP employee she suspects was involved in the privacy incident, I find that the applicant's motives in relation to her safety interests weigh heavily in favour of disclosure. Similarly, given the ongoing relationship between the applicant and CVAP, I also find that her motives as they relate to her privacy interests favour disclosure.

[170] Considering all these factors together, I find that they outweigh the s. 22(3)(d) presumption against disclosure. Given my finding that no factors weighed against disclosure, I find that it would not be an unreasonable invasion of Employee 1 and 2's personal privacy to disclose their personal information.

CONCLUSION

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

1. Subject to item 2 below, I confirm the Ministry's decision to refuse access to the information it withheld under s. 13(1).

2. The Ministry is not authorized under s. 13(1) to refuse access to the information that I have highlighted on page 100 in the copy of the records which is provided to the Ministry with this order. I require the Ministry to give the applicant access to the highlighted information.

3. Under s. 58(2)(b), I require the Ministry to reconsider its decision to refuse access to the information that I found it is authorized to withhold under s. 13(1). The Ministry is required to exercise its discretion and consider whether the s. 13(1) information should be released even though it is technically covered by the discretionary exception. It must deliver to the applicant the Ministry's reconsideration decision, along with the reasons and factors it considered for that decision and any additional information it decides to disclose.

4. I require the Ministry to give the applicant access to the information that it withheld under s. 22(1). That information is found on pages 98, 99, 103-104, 112-113, 120, and 126-131 of the records. These pages are indicated by yellow highlighting in the copy of the records which is provided to the Ministry with this order.

5. The Ministry must provide the OIPC Registrar of Inquiries with a copy of the Ministry's correspondence and the accompanying information sent in compliance with items 2, 3 and 4 above.

[172] Pursuant to s. 59(1) of FIPPA, the Ministry is required to comply with this order by **May 9, 2025**. Under s. 58(4), I require the Ministry to deliver the s. 13(1) reconsideration decision discussed at item 3 above to the applicant and the OIPC Registrar of Inquiries by this same date.

March 26, 2025

ORIGINAL SIGNED BY

Allison J. Shamas, Adjudicator

OIPC File No.: F23-93031