Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

Order F17-56

DELTA POLICE DEPARTMENT

Chelsea Lott
Adjudicator

December 14, 2017

CanLII Cite: 2017 BCIPC 61
Quicklaw Cite: [2017] B.C.I.P.C.D. No. 61

Summary: The applicants requested that the Delta Police Department (DPD) provide any records about themselves. DPD gave the applicants access to the responsive records but refused to disclose some information in them under s. 68.1(9) of the *Police Act* and ss. 14 (solicitor client privilege), 15(1)(e) (reveal criminal intelligence), 16(1)(b) (harm to intergovernmental relations) and 22 (harm to personal privacy) of the *Freedom of Information and Protection of Privacy Act*. The adjudicator confirmed DPD's decision to withhold information under s. 68.1(9) of the *Police Act,* and under ss. 14, 15 and 22. The adjudicator found that DPD properly withheld information pursuant to s. 16(1)(b), with the exception of one small excerpt. The adjudicator also ordered DPD to reconsider its exercise of discretion respecting a second small excerpt withheld under s. 16(1)(b). In addition, during the inquiry, the applicants asserted that s. 25 (disclosure of the information is in the public interest) of FIPPA applied. The adjudicator found that s. 25 did not apply.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, ss. 14, 15(1)(e), 16(1)(b), 22, 25; *Police Act*, s. 68.1(9)

Authorities Considered: B.C.: Order 02-38, 2002 CanLII 42472 (BC IPC); Order F15-30, 2015 BCIPC 33 (CanLII); Order 03-06, 2003 CanLII 49170 (BC IPC); Order F11-23, 2011 BCIPC 29 (CanLII); Order F16-14, 2016 BCIPC 16 (CanLII); Order 02-19, 2002 CanLII 42444 (BC IPC); Order F17-28, 2017 BCIPC 30 (CanLII); Order No. 331-1999, 1999 CanLII 4253 (BC IPC); Order 01-53, 2001 CanLII 21607 (BC IPC).

Cases Considered: *Rizzo & Rizzo Shoes Ltd. (Re)*, 1998 CanLII 837 (SCC); *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC); *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 (CanLII); *College of Physicians of BC v. British Columbia (Information and Privacy Commissioner)*, 2002 BCCA 665 (CanLII); *R. v. B.*, 1995 CanLII 2007 (BC SC); *Canada v. Solosky*, 1979 CanLII 9 (SCC); *R. v. Venneri*, 2012 SCC 33 (CanLII); *R. v. Saikaley*, 2017 ONCA 374 (CanLII); *R. v. Steele*, 2014 SCC 61 (CanLII); *John Doe v. Ontario (Finance)*, 2014 SCC 36 (CanLII).

Texts Considered: Peter Hogg, *Constitutional Law of Canada*, 5th ed. Supp. Toronto: Carswell, 2007; *Black's Law Dictionary*, 10th ed., by Brian A. Garner, ed. St. Paul, Minn.: Thomson Reuters, 2014; Sullivan, Ruth. *Sullivan on the Construction of Statutes*, 6th ed. Markham, Ont.: LexisNexis, 2014; *Canadian Oxford Dictionary*, 2nd ed., by Katherine Barber, ed. Don Mills, Ont.: Oxford University Press, 2004.

INTRODUCTION

[1] The applicants in this case were the subjects of an internal investigation by the Delta Police Department (DPD). One of the applicants is a former DPD employee and is in a relationship with the other applicant, who is not a DPD employee. The investigation was related to the applicant's employment with DPD and was not a criminal investigation. It centered on the applicants' alleged ties to organized crime and whether they posed a security threat to DPD.

[2] The applicants requested that DPD provide any records about themselves and consented to disclosing their own information to each other. DPD gave the applicants access to the responsive records but it withheld some information in them under ss. 14 (solicitor client privilege), 15 (harm to law enforcement), 16 (harm to intergovernmental relations) and 22 (harm to personal privacy) of the Freedom of Information and Protection of Privacy Act (FIPPA). DPD also withheld information on the basis that it was not responsive to the applicants' request.[1]

[3] The applicants disagreed with DPD's decision and requested a review by the Office of the Information and Privacy Commissioner (OIPC). During mediation, DPD reconsidered its decision and released some of the information it had previously withheld under s. 14. Mediation did not resolve the remaining issues and as a result, the OIPC issued a notice of inquiry to the applicants and DPD.

[4] During the inquiry, the applicants raised s. 25 (public interest) as an issue. DPD also reconsidered its decision to withhold information on the basis that it

[1] DPD also applied s. 15 to the information it deemed not responsive.

was not responsive to the applicants' request.[2] DPD disclosed further information and applied s. 22 to the names in the previously undisclosed information.[3]

[5] In addition, DPD raised s. 68.1(9) of the *Police Act* and requested that the OIPC provide notice of the inquiry to PrimeCorp, the Ministry of Public Safety and Solicitor General, the RCMP and all municipal police departments. The OIPC exercised its discretion under s. 54(b) of FIPPA to give notice of the inquiry to PrimeCorp, the Ministry, the British Columbia Association of Chiefs of Police (BCACP) and the BC Freedom of Information and Privacy Association (FIPA) and invited those parties to make submissions on s. 68.1(9) of the *Police Act*. All of those parties, except the Ministry, made submissions.

[6] Pursuant to the Commissioner's power to delegate under s. 49(1) of FIPPA, I have been given the power to conduct and decide this inquiry. However, DPD made a request pursuant to s. 49(1.1) that I not be given the power to examine certain excerpts in a police officer's notebook being withheld under s. 15. Section 49(1.1) reads:

> 49 (1.1) The commissioner may not delegate the power to examine information referred to in section 15 if the head of a police force or the Attorney General
>
> (a) has refused to disclose that information under section 15, and
>
> (b) has requested the commissioner not to delegate the power to examine that information.

[7] As a result, I have not considered the information which I am unable to examine and has been reviewed solely by the Commissioner. Any information which has been reviewed solely by the Commissioner pursuant to s. 49(1.1) does not form part of this order and is addressed in Order F17-57.

ISSUES

[8] The issues to be determined in this inquiry are as follows:

1. Does s. 68.1(9) of the *Police Act* exclude information from disclosure under FIPPA?

2. Is DPD required by s. 25 of FIPPA to disclose information in the public interest?

---

[2] At pp. 28, 44, 46, 49, 52, and 57-59 of the records.

[3] At pp. 46, 49, 52, and 59 of the records. DPD to date has not released the resevered records disclosing further information to the applicants despite direction by the OIPC to do so. In the context of this order, I have not considered the information which DPD has indicated it is no longer withholding because the issue is moot. It is expected that DPD will comply with its duties under FIPPA to disclose the newly severed records to the applicants without delay.

3. Is DPD authorized under ss. 14, 15 and/or 16 of FIPPA to refuse access to information?

4. Is DPD required to withhold information under s. 22 of FIPPA?

[9] Section 57 of FIPPA sets out the burden of proof regarding exceptions under FIPPA. DPD has the burden to establish that ss. 14, 15 and 16 authorize it to refuse to disclose information, and the applicants have the burden to establish that disclosure of any personal information would not unreasonably invade third party personal privacy under s. 22.

[10] Section 57 is silent on the burden of proof for s. 25. However I agree with the following statement from Order 02-38:

> Again, where an applicant argues that s. 25(1) applies, it will be in the applicant's interest, as a practical matter, to provide whatever evidence the applicant can that s. 25(1) applies. While there is no statutory burden on the public body to establish that s. 25(1) does not apply, it is obliged to respond to the commissioner's inquiry into the issue, and it also has a practical incentive to assist with the s. 25(1) determination to the extent it can.[4]

[11] Consistent with previous orders, DPD has the burden of establishing that the *Police Act* applies to exclude information from disclosure under FIPPA.[5]

DISCUSSION

Information in dispute

[12] The information in dispute is in records that relate to DPD's investigation of the applicants. The records include a memorandum, a report, handwritten notes, emails and printouts from various police databases as well as the internet. There are also emails between DPD employees and legal counsel respecting unrelated matters.

Police Act – s. 68.1(9)

[13] DPD says that some of the withheld information was acquired from the PRIME database and cannot be disclosed by virtue of s. 68.1(9) of the *Police Act*.

[4] Order 02-38, 2002 CanLII 42472 (BC IPC) at para. 39.
[5] Order F15-30, 2015 BCIPC 33 (CanLII) at para. 9; Order 03-06, 2003 CanLII 49170 (BC IPC) at para. 6.

Background

[14] The *Police Act* requires that all law enforcement services implement and use a common information management system, which is known by the acronym PRIME.[6] PrimeCorp is an emergency communications corporation registered pursuant to the *Emergency Communications Corporations Act*.[7] It provides operational and technical support for PRIME, as well as manages financial aspects of PRIME's operations.[8] PrimeCorp was designated as a public body under Schedule 2 of FIPPA in 2013.[9] The *Police Act* was later amended to add s. 68.1(9) to address access to information contained in PRIME.[10]

[15] The PRIME database provides many benefits for law enforcement. The database provides police with real time access to information about crimes, suspicious circumstances, investigations and police contact with the public.[11] More broadly, the technology promotes greater efficiency, accountability and investigational integrity for law enforcement.[12]

Statutory interpretation

[16] Personal information that law enforcement obtains through PRIME would, under FIPPA, ordinarily be in the custody or control of that law enforcement service and subject to access requests under FIPPA. The issue before me is whether s. 68.1(9) of the *Police Act* restricts access to information obtained by a law enforcement service through its access to PRIME. More specifically, the question is whether custody and control of information in PRIME can be transferred or shared between law enforcement services.

[17] This is the first time that s. 68.1(9) has been considered and interpreted by the OIPC. The modern approach to statutory interpretation requires that the words of an act be read in their entire context and in their grammatical and ordinary sense, harmoniously with the scheme of the act, the object of the act and the intention of the legislature.[13] Accordingly, it is appropriate to start by considering the purpose and legislative framework of FIPPA and the *Police Act*.

---

[6] PrimeCorp submissions at para. 7. PRIME stands for the Police Records Information Management Environment of British Columbia.
[7] SBC 1997 c. 47.
[8] PrimeCorp submissions at paras. 5-6.
[9] "PRIMECORP Police Records Information Management Environment Incorporated," was designated a public body by Ministerial Order No. M067 dated March 7, 2013.
[10] April 9, 2014.
[11] PrimeCorp submissions at para. 8.
[12] Appendix C, Operational Policy and Procedures Ch. 1.1.
[13] *Rizzo & Rizzo Shoes Ltd. (Re),* 1998 CanLII 837 (SCC) at para. 21.

FIPPA

[18] The purposes of FIPPA are set out in s. 2(1). Section 2(1) provides that one of FIPPA's purposes is "to make public bodies more accountable to the public." Subsections 2(1)(a) and 2(1)(c) provide that the purposes of FIPPA are accomplished by "giving the public a right of access to records" as well as by "specifying limited exceptions to the rights of access." The Supreme Court of Canada has considered the general purpose of access to information legislation in several cases and has long affirmed that access laws are of fundamental importance:

> The overarching purpose of access to information legislation, then, is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process, and secondly, that politicians and bureaucrats remain accountable to the citizenry.[14]

[19] FIPPA provides general rights of access to records which are in the custody or under the control of a public body. Section 3(1), which defines the scope of FIPPA, states:

> 3(1) This Act applies to all records in the custody or under the control of a public body …

[20] Section 4(1) of FIPPA incorporates the element of custody or control into the right of access to records:

> 4(1) A person who makes a request under section 5 has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.

[21] The public's general right of access to records is subject to enumerated exceptions contained in Division 2 of Part 2 of the Act.[15] Among the exceptions are discretionary exceptions wholly or partly relating to law enforcement information: ss. 15 (disclosure harmful to law enforcement) and 19 (disclosure harmful to individual or public safety). The purpose of the exceptions as they pertain to law enforcement are to protect public safety and ensure effective law enforcement.[16]

[22] Lastly, s. 79 of FIPPA sets out FIPPA's priority over other legislation where there is a conflict:

---

[14] *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC) at para. 61.
[15] The exceptions are contained in ss. 12-22.1.
[16] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 (CanLII) at para. 9, citing substantially similar provisions in Ontario's FIPPA.

> 79 If a provision of this Act is inconsistent or in conflict with a provision of another Act, the provision of this Act prevails unless the other Act expressly provides that it, or a provision of it, applies despite this Act.

Police Act

[23] The *Police Act* is the primary mechanism by which the province exercises its jurisdiction over the administration of justice.[17] Based on my review of the *Police Act*, I agree with PrimeCorp's characterization of the *Police Act* as "[the] statute that creates the framework for the delivery of police services in British Columbia and empowers the various police departments and other administrative bodies who carry out these functions."[18]

[24] I also agree with PrimeCorp's description of the general purpose of the *Police Act*, as "assuring the effective and efficient administrative of justice within the Province."[19]

[25] Turning to the section in issue, s. 68.1 requires law enforcement to use an information management system and provides the responsible minister the power to make regulations for all aspects of the implementation and operation of that system, being PRIME. The relevant portions are as follows:

> 68.1(1) In this section:
>
> "designated service provider" means a corporation that
>
> (a) is providing an information management system to a law enforcement service, and
>
> (b) is designated by order of the Lieutenant Governor in Council for the purposes of subsection (7);
>
> "information management system" means a system of software and hardware components and related technology that
>
> (a) interact and operate to integrate reception, creation, collection, recording, filing, analysis, reporting, transmission, storing, sending, reproduction and dissemination of information and data within and between policing and law enforcement jurisdictions, and
>
> (b) is approved by the minister under subsection (2);
>
> "law enforcement service" means the following:
>
> (a) the provincial police force;

[17] Peter Hogg, *Constitutional Law of Canada*, 5th ed. Supp. Toronto: Carswell, 2007 at 19-9.
[18] PrimeCorp submissions at para. 31.
[19] PrimeCorp submissions at para. 32.

> (b) a municipal police department;
>
> (c) any designated policing unit or designated law enforcement unit that is also designated by the minister as a law enforcement service for the purposes of this section;
>
> …
>
> (3) Subject to and in accordance with any regulation that may be made under section 74 (2)(v) or (x), a law enforcement service must implement, use, maintain, repair and upgrade an information management system approved by the minister.
>
> (4) For the purposes of this section, the minister may set or adopt standards to be followed by law enforcement services
>
> (a) respecting the manner, form, exchange and transfer of information and data in an information management system, and
>
> (b) for the maintenance of security and information and data integrity of an information management system.
>
> (5) A law enforcement service must comply with all standards set or adopted under subsection (4).
>
> …
>
> (9) If an information management system is provided by a designated service provider that is a public body under the *Freedom of Information and Protection of Privacy Act*,
>
> (a) the information and data in the information management system remain, for the purposes of that Act, in the custody and under the control of the law enforcement service from which the information and data originate, and
>
> (b) despite that Act, a person does not have a right of access under that Act to the information and data as being information and data in the custody or under the control of the designated service provider.

[26] PrimeCorp is a "designated service provider" and PRIME is an "information management system" for the purposes of s. 68.1.[20]

[27] It is against this legislative framework, that I turn to the interpretation of s. 68.1(9).

[20] Per Ministerial Order M70, March 10, 2005 and Order in Council 302, March 17, 2005 respectively.

Meaning of s. 68.1(9)

[28] DPD, BCACP and PrimeCorp all argue that s. 68.1(9) provides that custody and control of the information and data in PRIME lies solely with the originating law enforcement service. In other words, s. 68.1(9) precludes more than one law enforcement service from having custody or control of the same information in PRIME.

[29] FIPA's argument focuses on whether there is a right to access information contained in PRIME. FIPA submits that access requests to law enforcement should result in the release of responsive records in the custody or control of the public body as well as information which that public body has entered into PRIME. FIPA further argues that if the legislature wanted to exclude all information obtained through PRIME, it would have put in specific language to that effect.[21] In its view, s. 68.1(9) clarifies the method for making a request for information contained in PRIME, rather than restricting rights of access.[22]

[30] The applicants made no submissions regarding the interpretation of s. 68.1(9).

[31] As previously discussed, access to information under FIPPA is premised on a public body having custody or control of records. That is because s. 4(1) provides that, "[a] person who makes a request under section 5 has a right of access to any record in the custody or under the control of a public body…."[23] In my view, s. 68.1(9)(a) clearly acts to restrict the custody and control, and consequently access rights, to information contained in PRIME in the hands of law enforcement.

Section 68.1(9)(b)

[32] Although s. 68.1(9)(b) is not at issue in this case, I will address it for contextual purposes. Section 68.1(9)(b) states:

> (b) despite [FIPPA], a person does not have a right of access under [FIPPA] to the information and data as being information and data in the custody or under the control of the designated service provider.

[33] As a public body, PrimeCorp is subject to FIPPA, and the public has a right to request records from PrimeCorp. However, s. 68.1(9)(b) clearly places restrictions on that right of access. The public cannot access information and data in PRIME by requesting it from PrimeCorp.[24]

---

[21] FIPA submissions at paras. 17 and 19.
[22] FIPA submissions at para. 12.
[23] Section 4(1). See also s. 3(1).
[24] However, I note that this provision does not limit the public's right to access other types of records in the custody or under the control of PrimeCorp, such as its administrative records.

[34] DPD and PrimeCorp argue that s. 68.1(9)(b) means that PrimeCorp does not have custody or control of information in PRIME.[25] FIPA suggests that PrimeCorp does have custody or control of information and data in PRIME, but that s. 68.1(9)(b) means that the public cannot access it by making a request to PrimeCorp.[26]

[35] While I recognize that 68.1(9)(b) is somewhat ambiguous as to whether PrimeCorp has custody and control of information and data in PRIME, ultimately, I do not need to answer that question. That is because the applicants did not make their access request to PrimeCorp, rather it was made to DPD directly. Further, deciding whether PrimeCorp has custody and control of information and data in PRIME will make no practical difference in this case.

Section 68.1(9)(a)

[36] Section 68.1(9)(a) states:

> (a) the information and data in the information management system remain, for the purposes of that Act, in the custody and under the control of the law enforcement service from which the information and data originate

[37] The text of s. 68.1(9)(a) specifies that information and data "remain" in the custody and under the control of the law enforcement service from which the information and data originate. Law enforcement services frequently disseminate and share information with each other through PRIME. Therefore, the meaning of the "remain" is key to interpreting s. 68.1(9) and the legislature's intent regarding custody and control of information and data in PRIME.

[38] DPD cites two dictionary definitions of "remain" in support of its interpretation that s. 68.1(9) provides that custody and control of the information and data in PRIME lies solely with the originating law enforcement service.[27] Dictionaries can aid in determining the meaning of legislation.[28] The *Canadian Oxford Dictionary* defines "remain" *inter alia* as to "be in the same place or condition during further time; continue to exist or stay; be left behind." [29]

[39] Relying on the text of s. 68.1(9)(a) leads to an interpretation that custody and control of the information and data in PRIME stays, or is left behind, with the

---

[25] DPD initial submissions at para. 17. PrimeCorp submissions at para. 36.
[26] FIPA submissions at paras. 15-16.
[27] DPD initial submissions at paras. 16-17. Copies of the relevant portions of the dictionaries, the *Merriam Webster Dictionary* and the *Cambridge Dictionary*, were not provided, nor were citations provided. Accordingly, I have relied on the *Canadian Oxford Dictionary* which has a similar definition of "remain" as the dictionaries quoted by DPD.
[28] *R. v. Steele,* 2014 SCC 61 (CanLII) at paras. 42-44.
[29] *Canadian Oxford Dictionary*, 2nd ed., by Katherine Barber, ed. Don Mills, Ont.: Oxford University Press, 2004 at p. 1307.

originating law enforcement service after it has been entered into PRIME. It is as though the information never left the originating law enforcement service.

[40] Read together, the combined effect of ss. 68.1(9)(a) and (b) is to restrict the public's right to access data and information in PRIME to the law enforcement service which entered the information into PRIME.

[41] This interpretation is in line with the overall purpose of the *Police Act* which is ensuring the effective and efficient administrative of justice. One of the potential concerns with a multijurisdictional database is the accuracy and integrity of the information. To address this issue, PrimeCorp has made strict rules regarding supplementing files, and also prohibits an agency from amending, deleting or otherwise changing a record that has been contributed by another agency.[30] As PrimeCorp explains, the "police agency maintains control over its own investigation files…."[31] Section 68.1(9) enables law enforcement services to maintain the integrity of those files when an access request is made under FIPPA. That is because s. 68.1(9) ensures the investigating agency is the one which makes the decision about disclosure.

[42] In addition, the originating police agency would be in the best position to assess the application of exceptions under FIPPA. As BCACP explains:

> The police agency that creates information and contributes that information to PRIME-BC is in the best and likely the only position to properly assess access rights to that information. The originating investigative police agency has the benefit of context and detailed knowledge of its own file. The originating agency is the appropriate and only law enforcement service that can carefully and fully assess whether disclosure of its own information may be harmful to law enforcement (e.g. the file is under investigation; the file includes sensitive information that if disclosed is harmful to victims; the file includes information that if disclosed may be harmful to ongoing operations or intelligence).[32]

[43] I agree with BCACP's comments. In the sense that s. 68.1(9) promotes the informed and considered application of the exceptions under FIPPA, it supports one purpose of FIPPA. I would also add that FIPPA recognizes the importance of maintaining the integrity of law enforcement information. This is evidenced by exceptions which apply to law enforcement information such as ss. 15 (disclosure harmful to law enforcement), and 19 (disclosure harmful to individual or public safety).

---

[30] Appendix C Operational Policy and Procedures Ch. 4.2 and 5.2.
[31] PrimeCorp submissions at para. 33.
[32] BCACP submissions at p. 2.

Scope of information and data in PRIME

[44] Another interpretive question raised by s. 68.1(9)(a) is the scope of information captured by the provision. Section 68.1(9)(a) applies to "the information and data in the information management system." In the present case, the DPD has applied s. 68.1(9) to printouts from PRIME. However, it has also applied it to information that is not in its original format. For example, some information from PRIME has been handwritten into a police officer's notebook. Also, some of the information in the investigation report is in narrative format, but cites PRIME files as the source.

[45] In my view, changing the form of the information from a direct printout from PRIME to something else, does not take it outside the scope of s. 68.1(9) so long as it still reveals information in PRIME. It is important to note that s. 68.1(9) specifically refers to "information and data" as opposed to "records." This indicates that what is captured is the content of PRIME, regardless of its format. In other words, if the information at issue would reveal information contained in PRIME, then it is similarly subject to s. 68.1(9).

Overlap with FIPPA

[46] FIPA submits there is no conflict between s. 68.1(9) of *Police Act* and FIPPA because requests made to the originating law enforcement service should result in the release of records both in the hands of that agency as well as information that the agency entered into PRIME.[33] However, in my view, s. 68.1(9) restricts the information and access rights in s. 4 of FIPPA and in that sense, the provisions of the two statutes are in inconsistent or in conflict.

[47] In this case, the requested records and disputed information are in the physical possession of DPD and the applicants have made the request for access to DPD directly. If not for the restrictions that s. 68.1(9) sets regarding information in PRIME, the applicants would have the right - subject only to the operation of the exceptions to disclosure in FIPPA - to access the requested records in the custody or under the control of DPD. In short, s. 68.1(9) makes accessing information that a police department obtains from PRIME more onerous for access applicants; they cannot obtain the information directly from PrimeCorp and they must make their requests directly to the law enforcement services that originally put the information into PRIME.

[48] Section 79 of FIPPA provides that where FIPPA is "inconsistent or in conflict" with the provisions of another Act, FIPPA prevails unless the other Act, "expressly provides that it, or a provision of it, applies despite [FIPPA]." FIPA argues that s. 68.1(9) does not expressly provide that it prevails notwithstanding the provisions of FIPPA.[34] In my view, the wording of s. 68.1(9) is sufficiently

[33] FIPA submissions at para. 17.
[34] FIPA submissions at para. 18.

clear, and expressly provides, that the *Police Act* applies despite FIPPA. It is evident that the Legislature had FIPPA in front of mind when drafting s. 68.1(9) and intended for that provision to prevail despite FIPPA.

Application of s. 68.1(9) to the information

[49] DPD submits that it has applied s. 68.1(9) to information collected from PRIME and that the information originates from law enforcement services other than DPD.[35] In support of its submissions, DPD has provided affidavit evidence from one of the DPD constables involved in the investigation, (Constable S). He states that as part of his investigation, he searched PRIME for information about specific individuals. Constable S printed out lists of the events associated with those individuals and glued them into his notebook. He also wrote summaries in his notebook of the details of certain events.[36] DPD has also provided affidavit evidence from its PRIME administrator and system manager. She reviewed the records at issue, and deposes to the fact that some of them are direct print-outs from PRIME.[37]

[50] I am satisfied based on the above evidence as well as from my review of the records themselves, that all of the information to which DPD has applied s. 68.1(9) of the *Police Act* was information from PRIME and that it originated from other law enforcement services. The disputed information is clearly recognizable as originating from PRIME, because PRIME file numbers are cited. I find that DPD has properly withheld information which is not in its custody or control by virtue of s. 68.1(9).

[51] DPD is relying on s. 22(1) of FIPPA instead of s. 68.1(9) to withhold some information which it obtained from PRIME. As discussed below, I am satisfied that DPD is required to withhold that information pursuant to s. 22(1), so I have not considered the application of s. 68.1(9) to that information.

Public interest – s. 25

[52] Although s. 25 was listed as an issue in the notice of inquiry, neither party made submissions on its application. Section 25 overrides all of FIPPA's exceptions to disclosure, so I have considered it first in my analysis of FIPPA exceptions. Section 25 reads in part:

> 25 (1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people or to an applicant, information

[35] DPD initial submissions at paras. 14 and 19.
[36] Constable S affidavit at para. 6.
[37] PRIME system manager affidavit at paras. 7-12.

> (a) about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or
>
> (b) the disclosure of which is, for any other reason, clearly in the public interest.
>
> (2) Subsection (1) applies despite any other provision of this Act.

[53] Section 25(1)(a) applies where there is an imminent "risk of significant harm" to the environment or to human health or safety. The information in dispute here is plainly not about the matters described in s. 25(1)(a).

[54] Section 25(1)(b) only applies where disclosure is clearly in the public interest and the information concerns a matter justifying mandatory disclosure. As former Commissioner Denham explained in Investigation Report F16-02:

> There must be an issue of objectively material, even significant, public importance, and in many cases it will have been the subject of public discussion…disclosure must be plainly and obviously required based on a disinterested, reasonable, assessment of the circumstances.[38]

In my view, the information at issue here does not even remotely approach that standard of significant public importance. The applicants have not provided any evidence or argument to convince me otherwise. In conclusion, I find that s. 25 does not apply.

Solicitor client privilege – s. 14

[55] Section 14 of FIPPA 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 advice privilege and litigation privilege.[39] DPD submits that legal advice privilege applies to the information it is withholding under s. 14.

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

- there must be a communication, whether oral or written;
- the communication must be confidential;
- the communication must be between a client (or agent) and a legal advisor; and
- the communication must be directly related to the seeking, formulating or giving of legal advice.

---

[38] Investigation Report F16-02, *supra* at p. 36.
[39] *College of Physicians of BC v. British Columbia (Information and Privacy Commissioner)*, 2002 BCCA 665 (CanLII) at para. 26.

Not every communication between solicitor and client is protected by solicitor client privilege. However, if the four conditions above are satisfied, then legal advice privilege applies to the communications and the records relating to it.[40]

[57] DPD submits that the records deal with retaining counsel, questions from counsel, information provided to counsel and the interpretation or application of law.[41] DPD asserts that the records are specifically and solely communications with counsel to obtain legal advice, and are within the discretion of DPD to withhold under s. 14 of FIPPA.[42] The applicants provided no submissions respecting s. 14.

[58] I have reviewed the records to which DPD has applied s. 14. The affidavit of the inspector in charge of human resources (Inspector for Human Resources) accurately describes these communications. They are email communications between DPD's legal counsel and DPD's employees. The emails are between a small number of people, and some have explicit markings of confidentiality.[43] I have no difficulty in concluding that these emails, on their face, are directly related to the seeking, formulating or giving of legal advice. The emails concern matters related to the applicant's employment with DPD as well as the interpretation of legislation.[44] In sum, DPD has established all four of the requirements to satisfy legal advice privilege, and these records have been properly withheld under s. 14.

Harm to law enforcement – s. 15(1)(e)

[59] DPD submits that s. 15(1)(e) applies to portions of information it has withheld.[45] The information DPD has withheld under s. 15(1)(e) identifies third parties and their alleged connection to organized crime. The applicants provided no submissions on this exception.

[60] Section 15(1)(e) provides:

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

[40] *R. v. B.*, 1995 CanLII 2007 (BC SC) at para. 22. See also *Canada v. Solosky,* 1979 CanLII 9 (SCC) at p. 13.
[41] Records are at pp. 108-115. DPD initial submissions at para. 73.
[42] DPD initial submissions at para. 76.
[43] Pages. 108-113 of the records.
[44] Inspector of Human Resources affidavit at paras. 5 and 6.
[45] At pp. 9, 10, 16, 20-23 of the records. DPD also applied s. 15(1)(a) (harm to a law enforcement matter) to a small amount of information to which it applied s. 15(1)(e); however, as I have determined that DPD may withhold all of the information pursuant to s. 15(1)(e), I need not consider the application of s. 15(1)(a).

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

[61] This is the first time that the OIPC has considered s. 15(1)(e) at any length. Analysis of s. 15(1)(e) requires first determining whether the withheld information would reveal "criminal intelligence" and then considering whether that information has a reasonable connection with the prevention or suppression of organized criminal activities or of serious and repetitive criminal activities.

[62] The appropriate standard of proof for harms based exceptions, such as s. 15(1) which involve the wording "could reasonably be expected to" was stated by the Supreme Court of Canada in *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*:

> 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: paras. 197 and 199. 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.[46]

[63] DPD states that s. 15(1)(e) is not a harms based exception because of the legislature's choice of the verb "reveal" as opposed to other 15(1) subsections, which employ more active verbs specifically: "prejudice" "harm" "endanger" "deprive" and "facilitate." DPD also refers to the provincial government's *FOIPPA Policy and Procedures Manual*, which provides:

> [Section 15(1)(e)] does not require that harm be proven in order to withhold a record containing criminal intelligence. Due to the nature of criminal intelligence, it would normally not be possible to demonstrate that probable harm could result from disclosure of the intelligence. It could take months or years before the significance of the intelligence becomes apparent.[47]

---

[46] 2014 SCC 31 (CanLII) at para. 54.

[47] It can be found on the BC Government's website at: http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/foippa-manual. This manual was created and is maintained by the provincial government and it is not binding on the OIPC. However, it has been considered as an interpretive aid in previous OIPC orders. See: Order F11-23, 2011 BCIPC 29 (CanLII) at para. 19; Order F16-14, 2016 BCIPC 16 (CanLII) at para. 41.

[64] There is some confusion on the part of DPD about the meaning of "harms based" exceptions in FIPPA. In *Ontario (Community Safety and Correctional Services)*, the Supreme Court of Canada was quite clear that harms based exceptions are those which start with the wording "could reasonably be expected to," such as s. 15(1). The term "harms based" describes the standard of proof necessary for exemptions containing that wording. In the present case, the harm is the disclosure of criminal intelligence about specified criminal matters. The standard of proof requires evidence "well beyond" or "considerably above" a mere possibility of the harm happening.

[65] I agree with DPD that s. 15(1)(e) does not require any proof of additional future harm which could flow from disclosure of the information. The legislature has deemed simply revealing criminal intelligence as harm in and of itself.

[66] DPD's understanding of s. 15(1)(e) as not being a harms based exception may be due to the fact that some harms based exceptions contain the actual word harm. For instance s. 15(1)(a), which states, that a public body may refuse to disclose information that could reasonably be expected to "harm a law enforcement matter." However, it is the wording "could reasonably be expected to" which makes an exception a harms based exception - not the fact that the provision contains the word harm.

Criminal intelligence

[67] The phrase "criminal intelligence" is not defined in FIPPA. DPD argues that I should adopt the interpretation of "criminal intelligence" set out in the *FOIPPA Policy and Procedures Manual*, which states:

> "criminal intelligence" means information relating to a person or group of persons compiled by law enforcement agencies to anticipate, prevent or monitor possible criminal activity.
>
> Intelligence gathering is a separate activity from the conduct of investigations. Intelligence may be used for future investigations, for activities aimed at preventing the commission of an offence, and to ensure the security of individuals or organizations.[48]

[68] The phrase "criminal intelligence" is not defined in the *Canadian Oxford Dictionary*. However, it does provide other relevant definitions:

> "crime" is defined *inter alia* as "an offence punishable by law"
>
> "criminal" is defined *inter alia* as "of, involving or concerning crime"

[48] *Ibid*

> "intelligence" is defined *inter alia* as "the collection of information, especially of military or political value"[49]

[69] Similarly, "criminal intelligence" is not defined in *Black's Law Dictionary*, however it contains the following relevant definitions:

> "crime" is "[a]n act that the law makes punishable; the breach of a legal duty treated as the subject-matter of a criminal proceeding"
>
> "criminal" is *inter alia* "[o]f, relating to, or involving a crime; in the nature of a crime" [50]

[70] As previously discussed, the purpose of the law enforcement exceptions in access to information legislation is to protect public safety and ensure effective law enforcement.[51]

[71] Applying the dictionary definitions above suggests that "criminal intelligence" means the collection of information concerning crimes or activities punishable by law. However, in my view, that meaning is too broad. The plain meaning would capture information about investigations whereas FIPPA specifically differentiates between criminal intelligence and investigations. More specifically, FIPPA defines "law enforcement" as:

> (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;[52]

[72] It is presumed that the legislature avoids superfluous or meaningless words and that legislative provisions have their own meaning and function.[53] Accordingly, the legislature must have intended "criminal intelligence" to have a different meaning than "investigations" because they appear in discrete provisions of the definition of law enforcement. The context and surrounding language in s. 15(1)(e) is of assistance in determining what the legislature meant by "criminal intelligence":

---

[49] *Canadian Oxford Dictionary*, *supra* at pp. 358, 359 and 784.
[50] *Black's Law Dictionary*, 10th ed., by Brian A. Garner, ed. St. Paul, Minn.: Thomson Reuters, 2014 at pp. 451, 454-455.
[51] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 at para. 9, citing substantially similar provisions in Ontario's FIPPA.
[52] Schedule 1.
[53] Sullivan, Ruth. *Sullivan on the Construction of Statutes*, 6th ed. Markham, Ont.: LexisNexis, 2014 at §8.23.

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

[73] The use of the words detection, prevention or suppression, which are themselves ongoing or forward looking activities, suggests that criminal intelligence pertains to information about ongoing or possible future events. Restricting the meaning of "investigations" to past events, rather than ongoing or future events, avoids redundancy in the provisions of the definition for "law enforcement" in FIPPA because "investigations" and "criminal intelligence" would cover separate time frames.

[74] In light of the above considerations, I find that "criminal intelligence" in the context of s. 15(1)(e) means information collected by law enforcement to anticipate, or prevent crime. "Criminal intelligence" does not include law enforcement investigations into crimes that have allegedly already transpired.

[75] DPD submits that it is clear, based on the records and evidence, that the information in dispute would reveal "criminal intelligence."[54]

[76] I am satisfied that the information in dispute could reasonably be expected to reveal "criminal intelligence" within the context of FIPPA. From my review of the records, it is evident that the information itself is criminal intelligence. DPD has applied s. 15(1)(e) to information which identifies individuals with alleged gang connections. This information includes names, addresses, and gang affiliation. The information was obtained from PRIME or from Canadian Police Information Centre (CPIC), a national law enforcement database which is operated by the Royal Canadian Mounted Police.[55] DPD has also provided affidavit evidence from DPD's inspector in charge of DPD's criminal investigation branch (Inspector) who states that the information is of the type used to identify individuals involved in gang and organized criminal activity. The information at issue is clearly the type of information that law enforcement collects to anticipate, or prevent activities punishable by law.

Organized criminal activities

[77] The next step in the analysis under s. 15(1)(e) is to determine whether the criminal intelligence has a reasonable connection with the detection, prevention or suppression of organized criminal activities or of serious and repetitive criminal activities. DPD submits that it is clear from the records that the withheld information is specific to criminal or gang related associations and activities. The affidavit evidence of the Inspector states that the information DPD has withheld

[54] DPD initial submissions at para. 27.
[55] Pages 38, 46, 84-86, 92-94 and 103 of the records.

on pages 9 and 10 of the records is the type used by law enforcement to identify those individuals as being involved in particular gang and organized criminal activity, which is of a serious and repetitive nature.[56] The Inspector does not address the information to which DPD has applied s. 15(1)(e) on pp. 16, and 20–23.

[78] The terms "organized criminal activities" and "serious and repetitive criminal activities" are not defined in FIPPA. From my review of the records, it is clear that DPD withheld information about notorious criminal organizations which operate in BC. The withheld information states as much. These organizations fit within the stereotypical notion of organized crime. This is not to suggest that only information about stereotypical or notorious criminal organizations will meet the requirements of s. 15(1)(e); however whether a broader meaning of "organized criminal activities" is appropriate does not need to be considered in this case because of the infamy of the organizations involved.[57]

[79] I find support for the conclusion that the information relates to organized criminal activities in the investigation report which specifically states that its purpose was to determine the level, if any, of one of the applicant's "association with organized crime figures."[58] I also accept the Inspector's evidence that the information identifies individuals as being involved in particular gangs. It is evident from the record that this applies to all of the information which has been withheld under s. 15(1)(e) and not just the information on pages 9 and 10.

[80] I have no difficulty concluding that the information relates to "organized criminal activities" and that identifying who is associated with organized crime is necessary to detect, prevent or supress organized criminal activities. DPD has provided evidence that establishes that there is more than a mere possibility that disclosing the information in dispute could reasonably be expected to reveal the type of information captured by s. 15(1)(e). Accordingly, I am satisfied that DPD is authorized to withhold the information.

Harm to intergovernmental relations – s. 16(1)(b)

[81] The relevant portions of s. 16(1)(b) in this case are:

> 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:

[56] Inspector affidavit at para. 8.
[57] I note that the courts have adopted a broad definition of the related term "criminal organization" defined in s. 467.1(1) of the *Criminal Code*. See for example *R. v. Venneri*, 2012 SCC 33 (CanLII) and *R v. Saikaley*, 2017 ONCA 374 (CanLII).
[58] Page 8 of the records.

> (i) the government of Canada or a province of Canada;
>
> (ii) the council of a municipality or the board of a regional district;
>
> …
>
> (b) reveal information received in confidence from a government, council or organization listed in paragraph (a) or their agencies …
>
> (2) Moreover, the head of a public body must not disclose information referred to in subsection (1) without the consent of
>
> (a) the Attorney General, for law enforcement information, or
>
> (b) the Executive Council, for any other type of information.

[82] DPD has applied s. 16(1)(b) to information it obtained from CPIC. DPD has also withheld information in a report from the BC Combined Forces Special Enforcement Unit (CFSEU).[59] The applicants did not make any submissions respecting s. 16(1)(b).

[83] Section 16(1)(b) requires a public body to establish two things: that disclosure would reveal information it 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.[60]

[84] Previous orders have stated that s. 16(1)(b) is not a harms based exception.[61] However, it contains the reasonable expectation language, so in my view it is a harms based exception as outlined in *Ontario (Community Safety and Correctional Services)*.[62] As a result, the standard of proof for s. 16(1)(b) requires evidence well beyond or considerably above a mere possibility that disclosure would reveal information received in confidence from a government, council or organization listed in paragraph 16(1)(a) or their agencies.

CPIC records

[85] As previously mentioned, CPIC is a national law enforcement database operated by the RCMP. Previous BC Orders have established that the RCMP is a federal agency for the purpose of s. 16(1)(b).[63] Therefore, I need only consider whether DPD received the information in confidence from the RCMP.

---

[59] Pages 63-65 of the records.
[60] Order 02-19, 2002 CanLII 42444 (BC IPC) at para. 18.
[61] See for example Order F17-28, 2017 BCIPC 30 (CanLII) at para. 48.
[62] *Supra*
[63] Order 02-19, *supra* at para. 58.

[86] In Order No. 331-1999, former commissioner Loukidelis set out a non-exhaustive list of factors to determine whether information was received in confidence under s. 16(1)(b).[64] I have considered those factors below.

1. What is the nature of the information? Would a reasonable person regard it as confidential? Would it ordinarily be kept confidential by the supplier or recipient?

[87] I am satisfied that a reasonable person would regard the CPIC information as being confidential in nature. The records contain sensitive and potentially damaging personal information about individuals including gender, basic physical description, criminal record, gang affiliations, aliases, finger print codes, as well as cautionary warnings such as where someone is violent or poses an escape risk.

2. Was the record prepared for a purpose that would not be expected to require or lead to disclosure in the ordinary course?

[88] The CPIC information is not compiled for a purpose that would be expected to lead to disclosure, in the ordinary course, to the general public. The evidence establishes that CPIC information is available only to other law enforcement agencies and cannot be otherwise disclosed without permission of the contributing agency.

3. Do the records themselves contain explicit markings of confidentiality? Do the actions of the public body and the supplier of the record, provide objective evidence of an expectation of or concern for confidentiality?

[89] The CPIC records have explicit markings of confidentiality, as is evidenced by the CPIC records at pp. 97–103, which have been disclosed to the applicants.

[90] With respect to the actions of the public body, DPD has not consistently applied s. 16(1)(b) to CPIC records. DPD disclosed CPIC records regarding one of the applicants as well as information about an individual who has a similar name to the applicant.[65]

[91] Accordingly, there is some objective evidence of a concern for confidentiality, however I do not give these factors much weight because of DPD's inconsistent application of s. 16(1)(b).

---

[64] Order No. 331-1999, 1999 CanLII 4253 (BC IPC) at pp. 8-9.

[65] At pp. 97 to 103 of the records. On page 103, DPD has withheld part of that record which contains "RCMP Confidential finger print ID codes" according to an explanatory handwritten note on the record.

4. Was there an agreement or understanding between the parties that the information would be treated as confidential by its recipient?

[92] DPD argues that the information was received in confidence because the rules governing CPIC require an agency to obtain the permission of the originating agency to disclose the information.[66] The evidence of Constable S is that he has not obtained permission from the originating law enforcement agencies to disclose the information at issue.[67] DPD also provided evidence from its CPIC unit supervisor, who is DPD's primary liaison with the RCMP's CPIC management.[68] She states that CPIC's requirement that the originating agency approve any disclosure of information is fundamental to the integrity of CPIC.[69]

[93] DPD provided an excerpt from CPIC's policy manual. It contains the following relevant clauses:

> 11. CONFIDENTIALITY AND DISCLOSURE OF INFORMATION
>
> …
>
> 11.1.1. Information is entrusted to the CPI Centre for the purpose of communicating and sharing with the law enforcement and criminal justice community. There is a collective responsibility to ensure this information is safeguarded from improper and unauthorized access, use and disclosure…
>
> 11.1.1. Each Agency Head has a responsibility to ensure the confidentiality, safeguarding and authorized disclosure of the CPI Centre system information.
>
> …
>
> 11.2.1. The access, use and disclosure of any CPI Centre systems' information must:
>
> 11.2.1.1. be in accordance with existing federal, provincial, territorial or municipal legislation directives or policies related to privacy and access to information.… [70]
>
> 11.2.1.3 not be disclosed without prior confirmation and permissions from the originating agency…

[66] DPD initial submissions at para. 36.
[67] Constable S affidavit at para. 11.
[68] CPIC Unit Supervisor affidavit at para. 5.
[69] CPIC Unit Supervisor affidavit at para. 6.
[70] CPIC Unit Supervisor affidavit at exhibit A.

[94] Based on the foregoing evidence, I am satisfied that there was an understanding between the parties that the information would be treated as confidential by both the RCMP and DPD.

[95] I have no evidence on the remaining factors listed in Order 331-1999, so they are neutral in my analysis.[71]

[96] Weighing all of the above factors, DPD has satisfied me that it is considerably above a mere possibility that the information that DPD has withheld in the CPIC records was received in confidence within the meaning of s. 16(1)(b) and the exception applies to the information.

CFSEU record

[97] DPD has applied s. 16(1)(b) to withhold some information from a report it received from CFSEU. The report contains information about the applicants that appears to be derived from a variety of databases and online.

[98] Section 16(1)(b) requires that a public body establish that disclosure would reveal information it received from a government, council or organization listed in s. 16(1)(a) or one of their agencies. DPD submits that the withheld information was "provided by ICBC in confidence to the CFSEU, and further by the CFSEU in confidence to the DPD."[72] DPD submits that CFSEU and ICBC are agencies of the Province of British Columbia. However, I only need to consider whether CFSEU comes within s. 16(1)(a), because DPD received the information from CFSEU and not from ICBC.

[99] DPD submits that the report was "prepared by CFSEU, an agency of the Province of British Columbia in cooperation with the RCMP." Aside from this bald assertion, DPD has provided no evidence or case law to establish that CFSEU is an agency of the Province or that it otherwise fits within the entities described in s. 16(1)(a). The onus is on DPD to establish that the requirements of s. 16(1)(a) have been met. It has not done so regarding the CFSEU record. Therefore, I do not need to consider whether the information it received from CFSEU was received in confidence. I find that s. 16(1)(b) does not apply to the information withheld on pp. 63–65.

[71] The remaining factors are: (1) What is the past practice of the recipient public body respecting the confidentiality of similar types of information when received from the supplier or other similar suppliers? (2) Was the record supplied voluntarily or was the supply compulsory?
[72] DPD initial submissions at para. 47.

Disclosure Harmful to Personal Privacy - s. 22

[100] DPD is withholding some information under s. 22.[73] Numerous orders have considered the application of s. 22, and I will apply those same principles here.[74] The applicants have not made submissions on s. 22.

[101] DPD's investigation involved identifying third parties who had relationships with the applicants to determine whether the applicants had ties to organized crime. DPD has applied s. 22 to refuse to disclose all of the third party information, such as name, date of birth, driver's license information, photographs, and the nature of the individual's relationship with the applicants.

[102] Additionally, DPD has withheld police officer's home phone numbers[75] as well as information which identify third parties involved in unrelated investigations.

Personal information

[103] The first step in a s. 22 analysis is to determine if the information in dispute 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 telephone number, business address, business email or business fax number of the individual."[76]

[104] All of the information being withheld under s. 22 is personal information because it is about identifiable individuals and is not contact information. Most of it is third parties' personal information. However, where the information describes the nature of the relationship between the third party and one of the applicants, that is both the third party's and the applicant's information because it describes something about both individuals. None of the withheld information is solely the applicants' personal information.

Section 22(4)

[105] The next step in the s. 22 analysis is to determine whether the personal information falls into any of the types of information listed in s. 22(4). If it does, disclosure would not be an unreasonable invasion of personal privacy. From my review of the records, I am satisfied that DPD is not withholding any information which comes within s. 22(4).

---

[73] I have not considered the application of s. 22 to information that I have already found may be withheld under s. 16(1)(b), namely at pp. 84-86 and 92-94 of the records.
[74] See for example Order 01-53, 2001 CanLII 21607 (BCIPC) at p. 7.
[75] Page 49 of the records.
[76] See Schedule 1 of FIPPA for these definitions.

Presumptions

[106] The third step in the s. 22 analysis is to determine whether any of the s. 22(3) presumptions apply to the third party personal information. If so, disclosure is presumed to be an unreasonable invasion of privacy.

[107] DPD submits that the presumption against disclosure in s. 22(3)(b) applies to some of the information withheld under s. 22.[77] Section 22(3)(b) reads:

> 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, …

[108] DPD submits that the information to which it has applied s. 22(3)(b) consists of "personal information of third party individuals who were suspects, persons of interest, complainants, victims or witnesses in investigations into the circumstances surrounding possible violations of laws."[78]

[109] DPD relies on the records themselves as evidence.[79] In addition, DPD submits that any third party personal information which is obtained from PRIME or CPIC is subject to the presumption because law enforcement agencies contribute information "specific to investigations into possible or established violations of law."[80]

[110] I find that s. 22(3)(b) has been properly applied by DPD, based on my review of the records. The fact that the withheld information related to investigations into possible violations of law is discernable for the most part by the surrounding contextual information which has been disclosed to the applicants.

Relevant circumstances

[111] The fourth step in the s. 22 analysis is to consider the disclosure of the personal information in light of all relevant circumstances, including those in

---

[77] DPD has marked in the records "s. 22(3)(b)" next to information it alleges s. 22(3)(b) applies to at pp. 12, 13, 25, 46, 52 and 59 (as well as pp 84-86 and 92-94, which I have already found are subject to s. 16(1)(b) and so am not considering them in my s. 22 analysis).
[78] DPD initial submissions at para. 63.
[79] DPD initial submissions at para. 53.
[80] DPD initial submissions at para. 54.

s. 22(2). It is at this step that any presumptions may be rebutted. The factors listed in s. 22(2) that play a role in this case are as follows:

> 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,
>
> …
>
> (h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant …

[112] DPD submits that s. 22(2)(f) is a relevant consideration because the information was supplied in confidence. DPD argues:

> it is implicit in relation to, and as a result of the nature of police investigative activities and records, and it ought to reasonably be presumed, that individuals would expect their information to have been obtained or supplied in confidence, and that they would not want their names and other identifying information disclosed as appearing in investigative records specific to sensitive internally investigated police security matters….[81]

[113] The information at issue was not supplied by individuals directly to DPD rather, the information was supplied by the RCMP and PrimeCorp (through CPIC and PRIME databases). The issue is whether the RCMP and PrimeCorp supplied the information in confidence. I have previously held, in my findings regarding s. 16(1)(b), that the RCMP supplied the information confidentially to DPD. With regards to PrimeCorp, as discussed earlier in this order, the law enforcement services who utilize PRIME have detailed policies about adding, amending, deleting and disclosing information in PRIME. It is evident to me that information in PRIME is supplied confidentially to law enforcement services.

[114] Although not raised by DPD, I have considered s. 22(2)(h) which captures information which may unfairly damage the reputation of any person referred to in the record. The information at issue was compiled as a part of an internal workplace investigation by DPD. Much of it also contains allegations of criminal conduct by third parties. I conclude that disclosure of the third party personal information may unfairly damage the reputation of people referred to in the report. This is because the records contain unproven allegations and connect various third parties to criminal conduct. Further, the records do not include third

[81] DPD initial submissions at para. 58.

parties' responses, which are needed to counter-balance any negative impression given by this specific information.

Conclusion on s. 22(1)

[115] I have found that the presumption in s. 22(3)(b) applies to some of the withheld personal information. I have also considered s. 22(2)(f) and find that the personal information obtained through PRIME or CPIC was supplied in confidence. I also found that the circumstances addressed by s. 22(2)(h) are relevant here and weigh in favour of withholding the third party personal information. I can see no circumstances that weigh in favour of disclosing the third party personal information in this case. In balance, I find that disclosing the third party personal information would be an unreasonable invasion of third party personal privacy under s. 22(1).

[116] As previously discussed, some of the withheld information is both the applicants' and third parties' personal information. More specifically, I am referring to information about the nature of the relationships between the applicants and third parties, as well as a photograph of one of the applicants and a third party. It is rare that an applicant will be denied access to her or his own personal information in order to protect third party personal privacy.[82] However, I have also considered that disclosure of information through an access request is to be approached on the basis that it is disclosure to the world and not just to the applicants.[83] The applicants have the burden to establish that disclosure of any personal information would not unreasonably invade third party personal privacy under s. 22(1) and they have made no submissions on the exception. In this case, given the context of the information, as well as the potential unfair harm to third party reputations, I find that disclosure of information which is both the third parties' as well as the applicants' would be an unreasonable invasion of all of the third parties' personal privacy.

CONCLUSION

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

1. I confirm DPD's decision to refuse to give the applicants access to the information it withheld because of the application of s. 68.1(9) of the *Police Act*.

2. I confirm DPD's decision to refuse to give the applicants access to information under ss. 14 and 15(1)(e).

3. I confirm DPD's decision to refuse to give the applicants access to information under 16(1)(b) except for pages 63–65.

[82] Order 01-54, 2001 CanLII 21608 (BC IPC) at para. 26.
[83] Order 03-35, 2003 CanLII 49214 (BC IPC) at para. 31.

4. DPD is required to withhold all of the third party information that it refused to disclose to the applicants under s. 22.

I require DPD to give the applicants access to the information described in paragraph 3 by January 30, 2018. DPD must concurrently copy the OIPC Registrar of Inquiries on its cover letter to the applicants, together with a copy of the records.

December 14, 2017

ORIGINAL SIGNED BY

Chelsea Lott, Adjudicator

OIPC File No.: F15-63349