OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for British Columbia

Protecting privacy. Promoting transparency.

Order F15-72

MINISTRY OF PUBLIC SAFETY

Celia Francis
Adjudicator

December 23, 2015

CanLII Cite: 2015 BCIPC 78
Quicklaw Cite: [2015] B.C.I.P.C.D. No. 78

Summary: The applicant requested access to his BC Corrections file. The Ministry disclosed a number of records and withheld other records and information under ss. 15(1)(f), (g) and (l), 16(1)(b) and 22(1). The adjudicator found that ss. 15(1)(g), 16(1)(b) and 22(1) applied to some information and records. The adjudicator also found that ss. 15(1)(f) and (l) and s. 22(1) did not apply to other information and records and ordered the Ministry to disclose them.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, 15(1)(f), 15(1)(g), 15(1)(l), 16(1)(b), 22(1), 22(2)(e), 22(2)(f), 22(3)(b), 22(5)(a).

Authorities Considered: B.C.: Order No. 331-1999, 1999 CanLII 4600 (BC IPC); Order 00-02, 2000 CanLII 8819 (BC IPC); Order F08-03, 2008 CanLII 13321 (BC IPC); Order F10-39, 2010 BCIPC 59 (CanLII); Order F14-45, 2014 BCIPC 48 (CanLII); Order F15-55, 2015 BCIPC 58 (CanLII); Order 02-19, 2002 CanLII 42444 (BC IPC); Order F15-03, 2015 BCIPC 3 (CanLII); Order 01-37, 2001 CanLII 21591 (BC IPC); Order F14-10, 2001 CanLII 21561 (BC IPC); Order F08-02, 2008 CanLII 1645 (BC IPC); Order 01-07, 2001 CanLII 21561 (BC IPC); Order F12-14, 2012 BCIPC 12; Order F14-12, 2014 BCIPC 15 (CanLII); Order 01-52, 2001 CanLII 21606 (BC IPC); Order 03-24, 2005 CanLII 11964 (BC IPC); Order F10-41, 2010 BCIPC 61 (CanLII); Order F08-13, 2008 CanLII 41151 (BC IPC); Order F09-13, 2009 CanLII 42409 (BC IPC); Order F15-12, 2015 BCIPC 35.

Cases Considered: *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31; *Merck Frosst Canada Ltd. v. Canada (Health),* 2012 SCC 3; *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner*), 2012 BCSC 875.

INTRODUCTION

[1] The applicant in this case made a request to the Ministry of Justice ("Ministry"), under the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), for his BC Corrections file.[1] The Ministry responded by disclosing a number of records in full. It denied access to other records, in whole or in part, under s. 15(1) (harm to law enforcement), s. 16(1) (information received in confidence) and s. 22(1) (harm to third-party privacy). The applicant requested a review of the Ministry's response by the Office of the Information and Privacy Commissioner ("OIPC"). Mediation by the OIPC resulted in the disclosure of some more information[2] but was not otherwise successful. The matter then proceeded to an inquiry. The OIPC received submissions from the Ministry and the applicant.

ISSUES

[2] The issues before me are these:

1. Whether the Ministry is authorized by ss. 15(1) and 16(1) of FIPPA to refuse access to the requested information.
2. Whether the Ministry is required by s. 22(1) of FIPPA to refuse access to the requested information.

[3] Under s. 57(1) of FIPPA, the public body has the burden of proving that the applicant has no right of access to all or part of the requested records, under ss. 15 and 16, including portions of the records that contain the applicant's own personal information. Under s. 57(2), the applicant has the burden of proving that disclosure of third-party personal information would not be an unreasonable invasion of the third party's personal privacy under s. 22(1).[3]

DISCUSSION

Background

[4] The BC Corrections Branch is part of the Ministry. It provides correctional services and programs to people who are 18 and older who are (1) supervised while on bail awaiting trial or serving a community sentence or (2) held in custody while awaiting trial or serving a jail sentence of less than two years. When

[1] Responsibility for BC Corrections was assigned to the Ministry of Public Safety in mid-December 2015. This order is therefore directed at the Ministry of Public Safety.
[2] Paragraph 4.03, Ministry's initial submission.
[3] See Order No. 331-1999, 1999 CanLII 4600 (BC IPC), at pp. 3-4, and Order 00-02, 2000 CanLII 8819 (BC IPC), at p. 3, where former Commissioner Loukidelis discussed the general burden of proof in s. 57(1) on the public body, including with respect to the applicant's own personal information, and the burden of proof in s. 57(2) on the applicant respecting third-party personal information.

supervising offenders in the community, community corrections staff interact with offenders, victims, police, crown counsel, court staff and community agency partners. They also conduct risk assessments and make recommendations to the court to assist with sentencing decisions. Probation officers conduct in-person visits and electronic monitoring and make sure offenders comply with the terms of their court-ordered supervision.[4]

[5] Under s. 1(2) of the *Attorney General Act*, the Attorney General is responsible for the management and direction of the Ministry, including the conduct of prosecutions in British Columbia.[5] The Criminal Justice Branch ("CJB") has a number of responsibilities and functions under the *Crown Counsel Act*, including approving and conducting all prosecutions within the province, and initiating and conducting all appeals and other proceedings respecting any prosecution. Crown counsel in the CJB are responsible for conducting prosecutions under the direction of the Assistant Deputy Attorney General.[6]

Records in dispute

[6] The withheld information and records include the following:

- BC Corrections Branch – Client Log
- BC Corrections Branch – Contact Recording Sheets
- Letters and fax cover sheets
- Community Risk Needs Assessments
- Home Visit Reports
- Interim Summaries
- Supervision Orders
- Reports to Crown counsel, which include narratives, witness lists and witness statements
- Canadian Police Information Centre ("CPIC") printouts

Harm to law enforcement – ss. 15(1)(f), (g) and (l)

[7] The Ministry argued that ss. 15(1)(f), (g) and (l) apply to some of the information and records in dispute. These provisions read as follows:

[4] Paragraphs 4.07-4.11, Ministry's initial submission; paras. 3-8, Clarke affidavit.
[5] Paragraphs 4.01-4.02, Ministry's initial submission.
[6] Paragraphs 4.12-4.16, Ministry's initial submission.

Disclosure harmful to law enforcement

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

…

(f) endanger the life or physical safety of a law enforcement officer or any other person,

(g) reveal any information relating to or used in the exercise of prosecutorial discretion,

…

(l) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

Standard of proof for harms-based exceptions

[8] I will begin by considering the Ministry's arguments that harm could reasonably be expected to flow from disclosure of the information it withheld under ss. 15(1)(f) and (l). The Supreme Court of Canada in *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)* said the following regarding the standard of proof for harms-based provisions:

> 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".[7]

[9] Moreover, in *British Columbia (Minister of Citizens' Services) v. British Columbia (Information and Privacy Commissioner)*,[8] Bracken J confirmed it is the release of the information itself that must give rise to a reasonable expectation of harm and that the burden rests with the public body to establish that the

[7] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31, at para. 54, citing *Merck Frosst Canada Ltd. v. Canada (Health),* 2012 SCC 3, at para. 94.
[8] 2012 BCSC 875, at para. 43.

disclosure of the information in question could reasonably be expected to result in the identified harm.

[10] In assessing the Ministry's arguments of harm under ss. 15(1)(f) and (l), I have taken the approach as set out above and in previous orders and court decisions.[9]

Endanger life or safety – s. 15(1)(f)

[11] The Ministry submitted that information may be withheld if it could reasonably be expected to "heighten an already prevalent risk to the physical safety of a law enforcement officer or other person, even if such harm never occurs or if such harm is not likely to occur". The Ministry noted that the applicant has a history of "assaultive behaviour", with the most recent charge for assault in 2013. It said that many of the applicant's charges involved individuals with whom the applicant had "an ongoing or close and personal relationship". It argued that disclosure of the information it withheld under s. 15(1)(f) could reasonably be expected to "incite the Applicant leading to altercations endangering the individuals named in the records" who, it said, are "accessible within the community". The Ministry submitted some *in camera* affidavit evidence on this point.[10] The applicant did not address s. 15(1)(f).

[12] The information in issue respecting s. 15(1)(f) is a sentence in a page of handwritten "opinion notes"[11] and two handwritten paragraphs in "Contact Recording Sheets Comments" ("contact sheets").[12] All the information was recorded in the mid-1990s.

[13] In the open part of its affidavit evidence, the Ministry described this withheld information as "opinions".[13] I agree with this description and would add that, in my view, because the opinions are about the applicant, they are the applicant's personal information.

[14] The already disclosed records and information show that the applicant has a history of charges, including for assault, going back to 1993. As far as I can tell, the assault charges relate primarily, if not entirely, to women with whom the applicant has had an intimate relationship. There is no indication in the records that the applicant has had a "close and personal relationship" with the individuals named in the records about whom the Ministry expressed concern. There is also no indication that he has behaved violently to them. I also note that the Ministry

[9] See also, for example, Order F08-03, 2008 CanLII 13321 (BC IPC), Order F10-39, 2010 BCIPC 59 (CanLII), and Order F14-45, 2014 BCIPC 48 (CanLII).
[10] Paragraphs 5.04-5.09, Ministry's initial submission; paras. 26-27, Clarke affidavit.
[11] Page 154.
[12] Pages 139 and 145, second withheld passage.
[13] Paragraph 27, Clarke affidavit.

has already disclosed some information that BC Corrections staff provided that describes recent hostile, argumentative and rude behaviour by the applicant.[14] There is no evidence that disclosure of this information has exposed these employees to harm for the purposes of s. 15(1)(f).

[15] As noted above, a public body must "establish a clear and direct connection between the disclosure of the withheld information and the alleged harm."[15] The Ministry did not, however, describe what it calls the "already prevalent risk to the physical safety" of individuals. Nor did it explain how disclosure of this 20-year-old information could "incite the Applicant leading to altercations endangering the individuals" in question. The Ministry's evidence and argument regarding s. 15(1)(f) are speculative, in my view, and amount to little more than assertions. They fall short of the "detailed and convincing" evidence that past orders and court cases have said is required to establish harm under s. 15(1). The Ministry has not, in my view, met its burden of proving that disclosure of this information could reasonably be expected to endanger the life or physical safety of a law enforcement officer or any other person. I find that s. 15(1)(f) does not apply to the information which the Ministry withheld under this provision. However, the Ministry applied s. 22 to this information as well, so I will address it further below.

Harm security of property or system – s. 15(1)(l)

[16] The Ministry withheld two types of information under this section: "employee user identifiers" and "risk assessment classifications" of the applicant. It did not apply any other exceptions to this information. The applicant did not address s. 15(1)(l) and whether disclosure of the information to him could reasonably be expected to harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.

[17] Employee user identifiers: The Ministry argued that disclosure of the identifiers would give hackers "valuable information to assist in breaching layers of security of government systems to access extremely sensitive corrections information". The Ministry provided affidavit evidence on this point from Gary Perkins, Chief Information Security Officer and Executive Director of the Information Security Branch, Ministry of Technology, Innovation and Citizens' Services, the essence of which is this:

- access to user identifiers would increase the chances of hackers successfully attacking and compromising government computer systems

[14] See, for example, entry on p. 9 dated 2013.02.21 at 12:35:50; entry on p. 10 dated 2013.05.15 at 14:43:35.
[15] See also Order F08-03, 2008 CanLII 13321 (BC IPC), at para. 27.

- without valid user identifiers, hackers would have to guess both user identifiers and passwords, decreasing their chances of successfully attacking government computer systems, because of the significant increase in the combinations of user identifiers and passwords they would have to try[16]

[18] Section 15(1)(l) explicitly refers to harm to security of a "computer system". I am therefore satisfied that the government computer system is a "system" for the purposes of s. 15(1)(l).

[19] As for the alleged harm to this system on disclosure of the type of information in issue here, in Order F14-12,[17] Adjudicator Flanagan rejected a similar argument, noting, among other things, that access to an employee's password and additional expertise would be needed to gain unauthorized access to the computer system in question. I am similarly not persuaded that the "system" in this case could be compromised by disclosure of the user identifiers. For one thing, as the Ministry itself acknowledges, there are security controls in place to mitigate risks to the compromise of government computer systems (*e.g.*, password complexity; temporary account lockout after five unsuccessful tries).[18] The Ministry also admitted that system administrators are able to detect attempts at unauthorized access to government computer systems.[19]

[20] Moreover, while the Ministry's submission primarily concerned unauthorized access to government-wide systems,[20] its evidence suggests that the employee user identifiers in issue here are used to log on to the BC Corrections system only.[21] If so, the Ministry did not explain how a hacker might use unauthorized access to the BC Corrections system to gain unauthorized access to computer systems government-wide.

[21] In addition, the Ministry said knowledge of user identifiers would make it "half again as likely" that a hacker would be successful in bypassing security controls to gain unauthorized access to government systems.[22] "Half again as likely" as what, it did not say.

[22] In my view, the Ministry's arguments are speculative and it has not established that the disclosure of the information in question could reasonably be expected to result in the identified harm. As former Adjudicator McEvoy said in Order F10-39, it is not credible to conclude that the government's computer

[16] Perkins affidavit.
[17] 2014 BCIPC 15 (CanLII), at para. 18.
[18] Paragraph 19, Perkins affidavit.
[19] Paragraph 30, Perkins affidavit.
[20] Perkins affidavit.
[21] Paragraph 35, Clarke affidavit.
[22] Paragraph 11, Perkins affidavit.

systems are that "fragile".[23] For the reasons given above, I find that s. 15(1)(l) does not apply to the employee user identifiers.

[23] Risk assessment information: The Ministry said this information discloses the level of risk at which the applicant, as an offender, has been assessed, the factors leading to this assessment and thus the level of his supervision, and that disclosure could therefore reasonably be expected to harm BC Corrections' "operations". The applicant did not address this issue.

[24] The Ministry's argument and evidence on this point may be summarized as follows:

- an offender could "skew the results" of his assessment to his benefit, for example, to ensure he was subject to a lower level of supervision
- risk assessments also affect how and where corrections officers interact with offenders (*e.g.*, only where there is a glass barrier between the offender and staff)
- if risk assessment results were improperly altered, an offender could receive a "better" assessment, which would harm the security of correctional centres and of Community Corrections Branch's operations, which act in a less secure setting than correctional centres
- community corrections staff have been assaulted by individuals being supervised in the community
- improper alterations in risk assessments would also affect corrections staff's ability to make accurate recommendations to the Court about the offender[24]

[25] The information in issue here is "about" the applicant and it is thus his personal information. The question is, would disclosure of the applicant's risk assessment information reasonably be expected to harm the security of property or systems for the purposes of s. 15(1)(l)? For reasons given below, the Ministry has not persuaded me that such harm could reasonably be expected to occur.

[26] The examples that s. 15(1)(l) lists for "property" are "a building or a vehicle". Past orders have found that jails are "properties" for the purposes of s. 15(1)(l).[25] I also accept that s. 15(1)(l) may be applied to protect the security of properties such as community corrections offices.

[27] The examples that s. 15(1)(l) lists for "system" are "a computer system or a communications system". Past orders have found that a "system" includes

[23] Order F10-39, 2010 BCIPC 59 (CanLII), at para. 17.
[24] Paragraphs 5.18-5.21, Ministry's initial submission; paras. 36-45, Clarke affidavit.
[25] See for example, Order F08-13, 2008 CanLII 41151 (BC IPC), at para. 43.

a video surveillance system, a teleconferencing system and a public transportation system.[26]

[28] The Ministry's submission was directed to possible harm to "BC Community Corrections operations". It did not, however, explain how "BC Community Corrections operations" are a "system" for the purposes of s. 15(1)(l). It seems to me that the BC Corrections operations are more properly a "program". Moreover, the Ministry's concerns over the compromising of these "operations" and consequent potential risk to employees, in my view, relate more properly to s. 15(1)(f) than s. 15(1)(l).

[29] Even if I do accept that BC Corrections operations are a "system" for the purposes of s. 15(1)(l), the Ministry has not persuaded me that disclosure of the risk assessment information could reasonably be expected to cause the anticipated harm to this "system" – or to the Community Corrections offices, for that matter. For one thing, I note that the information in question relates to assessments by Community Corrections staff who supervised the applicant in 1995-1996. The Ministry did not say if it still considers these risk assessments to apply to the applicant. Nor did it say if it still uses the same kind of assessment tools and ratings as it did in the mid-1990s. The Ministry also did not explain how the withheld information reveals factors leading to the applicant's risk assessment and thus the level of his supervision. These details are not evident from the information in question.

[30] Moreover, the Ministry's position on s. 15(1)(l) is speculative, in my view, and directed more at offenders generally, rather than the applicant. The Ministry did not, for example, cite cases where offenders had insincerely changed their behaviour for the better as a result of knowing their risk assessments, resulting in harm for the purposes of s. 15(1)(l). In any case, the records indicate that BC Corrections staff have given the applicant advice over the years on how to behave appropriately, so it seems to me that the applicant is already aware of how he could alter his risk assessment for the better.

[31] The Ministry also argued that the assessment of harm in this case should take into consideration that disclosure under FIPPA is effectively disclosure to the world. It argued that, therefore, disclosure of the risk assessment information to the applicant would be disclosure to "those with malicious intent to subvert community corrections systems".[27]

[32] I do not agree with the Ministry on this point. The "disclosure to the world" argument applies to general information, not personal information.[28] The

[26] See for example, Order F08-13, 2008 CanLII 41151 (BC IPC), at para. 43, and Order F09-13, 2009 CanLII 42409 (BC IPC), at paras. 13-17, Order F14-12, 2015 BCIPC 35, at para. 12.
[27] Paragraph 5.22, Ministry's initial submission.
[28] See Order 01-52, 2001 CanLII 21606 (BC IPC), at para. 73.

applicant's risk assessments are his personal information. Disclosure of the applicant's own personal information to him does not mean that others would also be entitled to it. Even if this information did fall into the hands of others, it would be of little or no use to them, as it pertains to the applicant, and I see no broader usefulness to anyone intent on causing harm.

[33] For reasons given above, I find that the Ministry has not met its burden of proving that the applicant is not entitled to his own personal information and that s. 15(1)(l) does not apply to the risk assessment information in question.

Exercise of prosecutorial discretion – s. 15(1)(g)

[34] The Ministry argued that s. 15(1)(g) applies to the Reports to Crown Counsel ("RCCs") and to some other information[29] because disclosing them could reasonably be expected to reveal information relating to or used in the exercise of prosecutorial discretion.

[35] The relevant part of the definition of "exercise of prosecutorial discretion" in Schedule 1 of FIPPA reads as follows:

> **"exercise of prosecutorial discretion"** means the exercise by
>
> (a) Crown counsel, or a special prosecutor, of a duty or power under the *Crown Counsel Act*, including the duty or power
>
> (i) to approve or not to approve a prosecution,
>
> (ii) to stay a proceeding,
>
> (iii) to prepare for a hearing or trial,
>
> (iv) to conduct a hearing or trial,
>
> (v) to take a position on sentence, and
>
> (vi) to initiate an appeal, or
>
> …

Parties' submissions on s. 15(1)(g)

[36] The Ministry said that some of the information, including the RCCs, was provided to the CJB for the purposes of deciding whether or not to approve the prosecution relating to the applicant and whether to bring him back before the Court for a review of his conditions while on bail or probation. The Ministry said that the information was also used in Crown counsel's ongoing assessment of whether to continue the prosecution, including while the applicant was on probation. The Ministry provided a letter in support of its position from

[29] Page 128, middle entries; p. 133, bottom entry; p. 134, bottom entry; p. 135, third entry; p. 149, only entry; pp. 162, 164-180.

Lori McMorran, Information Access and Privacy Coordinator/Crown Counsel, CJB.[30]

[37] The applicant provided a brief submission which appeared to relate to an RCC regarding an incident involving his former wife in 2013, which was the record in dispute in Order F15-55.[31] He also provided an affidavit from his former wife consenting to the disclosure of the RCC and her statement to the RCMP in that case.[32]

Analysis of s. 15(1)(g)

[38] Portions of the Report to Crown counsel that I considered in Order F15-55 are in issue in this case as well.[33] I found in Order F15-55 that s. 15(1)(g) applied to them, so I need not consider them again here.

[39] As for the remaining information and records withheld in this case under s. 15(1)(g), I am satisfied by the Ministry's evidence that Crown counsel reviewed and considered them in exercising discretion in deciding whether to lay criminal charges against the applicant. I find that s. 15(1)(g) applies to that information and records. I include here the last seven lines of the withheld passage on page 150, which is similar in character to the information which the Ministry withheld elsewhere under s. 15(1)(g), but to which the Ministry did not apply s. 15(1)(g). (It applied s. 22 only.)

[40] I find support for my conclusion in Order 00-02, in which former Commissioner Loukidelis had evidence that Crown counsel had used an RCC and other records in deciding whether to lay charges against an applicant. He found that s. 15(1)(g) applied to the records.[34]

Exercise of discretion regarding s. 15(1)(g)

[41] While I have found that s. 15(1)(g) applies to the records and information in issue in this case, this is not the end of the matter. Section 15(1)(g) is a discretionary exception, so the Ministry must consider the relevant factors in exercising its discretion in favour of withholding or disclosing the requested records.[35]

---

[30] Clarke affidavit, paras. 28-33; McMorran letter, Exhibit C, Clarke affidavit.
[31] 2015 BCIPC 58 (CanLII).
[32] Applicant's submission. The wife's statement was part of the Report to Crown Counsel in that case.
[33] Pages 165-168 and 170.
[34] 2000 CanLII 8819 (BC IPC), at p. 4.
[35] See Order 00-02, 2000 CanLII 8819 (BC IPC), at p. 5, for a discussion of the factors public bodies should consider in the exercise of discretion in relation to s. 15(1)(g), which include whether the records have already been disclosed under criminal law disclosure rules.

[42] In this case, the Ministry said it considered the fact that some of the records had already been disclosed to the applicant in the context of criminal proceedings. The Ministry argued that, if the applicant received the records under FIPPA, however, he would not be bound, as he was in the criminal proceeding, by an implied undertaking not to further use or disclose them and the records would not be subject to judicial controls limiting their use. The Ministry said it had also considered the sensitivity and nature of the records, the purpose of the exception and whether there is a sympathetic or compelling need to disclose the records. The Ministry said it had also considered the former wife's consent to disclosure, but argued, for a number of reasons, that her consent was not informed consent.[36]

[43] I am satisfied that the Ministry considered appropriate factors in deciding to withhold the RCC under s. 15(1)(g) and the Ministry properly exercised its discretion.

Conclusion on s. 15(1)

[44] I found that ss. 15(1)(f) and 15(1)(l) do not apply to the records and information in dispute. However, I found that the Ministry has met its burden of proof regarding s. 15(1)(g) and that it exercised its discretion properly in withholding the information in question in these records.[37]

Information received in confidence – s. 16(1)(b)

[45] The Ministry said that it received some of the information and records in confidence from the RCMP and that s. 16(1)(b) therefore applies to them. The applicant did not address this issue.

[46] I found above that s. 15(1)(g) applies to some of the same information and records to which the Ministry applied s. 16(1)(b). So, I need not also consider if s. 16(1)(b) applies to the same items.[38]

[47] The relevant provisions read as follows:

> **Disclosure harmful to intergovernmental relations or negotiations**
>
> 16(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

[36] Paragraphs 5.32-5.34, Ministry's initial submission; Clarke affidavit, para. 53; Ministry's reply submission.
[37] Page 128, middle entries; p. 133, bottom entry; p. 134, bottom entry; p. 135, third entry; p. 149, only entry; last seven lines of the withheld passage on p. 150; all of pp. 162, 164-180.
[38] Page 149, only entry; all of pp. 166-170, 175-180.

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

Standard for applying s. 16(1)(b)

[48] Former Commissioner Loukidelis established a two-part test for the application of s. 16(1)(b) in Order 02-19.[39] The first part is to determine whether the information was supplied by one of the bodies listed in s. 16(1)(a) or any of their agencies. The second part of the test is to determine whether the information was "received in confidence". In Order No. 331-1999,[40] the former Commissioner considered the meaning of the phrase "received in confidence". He expressed the view that there must be an implicit or explicit agreement or understanding of confidentiality on the part of both those supplying and receiving the information. He also set out several relevant circumstances that public bodies should consider in determining if information "was received in confidence".

Ministry's submission

[49] The Ministry said that its Corrections Branch received CPIC printouts and other information being withheld under s. 16(1)(b) in confidence from the RCMP for the purpose of supervising the applicant while he was on probation or bail. Corporal Dean R. Allchin of the RCMP provided an affidavit in support of the Ministry's submission on the confidentiality issue.[41]

Analysis

[50] I find that the RCMP are an "agency" for the purposes of s. 16(1)(a). This is also what former Commissioner Loukidelis found in Order 02-19.[42] The Ministry's submission also satisfies me that appropriate indicators of confidentiality are present. I find as follows:

---

[39] 2002 CanLII 42444 (BC IPC), at para. 58.
[40] 1999 CanLII 4253 (BC IPC), at pp. 6-9.
[41] Paragraphs 5.41-5.46, Ministry's initial submission; Clarke affidavit, paras. 46-52; Allchin affidavit.
[42] 2002 CanLII 42444 (BC IPC), at para. 58.

- the information is of a nature that a reasonable person would consider confidential
- the RCMP provided the information and records in confidence, with the expectation that they would be treated as confidential
- the Ministry has consistently treated the information in confidence
- the Ministry has a Memorandum of Understanding with the RCMP which provides for restrictions on the further use and dissemination by the Ministry of the RCMP information and records

[51] For these reasons, I find that s. 16(1)(b) applies to the information and records in question.

Exercise of discretion

[52] The Ministry said it considered a number of factors in exercising its discretion to apply s. 16(1)(b), including some listed above under s. 15(1)(g).[43] The Ministry's submission also indicates that it is important for it to maintain its working relationship with the RCMP, in which sensitive information is exchanged on a confidential basis.[44] In my view, these are appropriate factors to consider and I find that the Ministry exercised its discretion properly in deciding to apply s. 16(1)(b).

Conclusion on s. 16(1)(b)

[53] I found above that s. 16(1)(b) applies to the information and records in issue here and that the Ministry exercised its discretion properly in deciding to apply s. 16(1)(b) to them.[45] I find that the Ministry has met its burden of proof regarding s. 16(1)(b) in this case.

Harm to third-party personal privacy

[54] The Ministry submitted that disclosure of some of the information would be an unreasonable invasion of third-party privacy under s. 22(1) of FIPPA. The applicant did not address s. 22(1) except in the context of the records to which I found above s. 15(1)(g) applies. I need not consider any of the information that I found, above, could be withheld under s. 15(1)(g) and/or s. 16(1)(b).[46]

---

[43] Clarke affidavit, para. 53.
[44] Ministry's initial submission, para. 5.44.
[45] Page 7, middle entry; all of pp. 157-161.
[46] Page 7, middle entry; p. 134, bottom entry; p. 135, third entry; pp. 149; last seven lines of withheld information on p. 150; pp. 166-168, 170, 172, 174-180.

Approach to applying s. 22(1)

[55] The approach to applying s. 22(1) of FIPPA has long been established. See, for example, Order F15-03:

> Numerous orders have considered the approach to s. 22 of FIPPA, which states that a "public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy." This section only applies to "personal information" as defined by FIPPA. Section 22(4) lists circumstances where s. 22 does not apply because disclosure would not be an unreasonable invasion of personal privacy. If s. 22(4) does not apply, s. 22(3) specifies information for which disclosure is presumed to be an unreasonable invasion of a third party's personal privacy. However, this presumption can be rebutted. Whether s. 22(3) applies or not, the public body must consider all relevant circumstances, including those listed in s. 22(2), to determine whether disclosing the personal information would be an unreasonable invasion of a third party's personal privacy.[47]

[56] I have taken the same approach in considering the s. 22 issue here.

Is the information "personal information"?

[57] FIPPA defines "personal information" as recorded information about an identifiable individual, other than contact information.[48] The Ministry argues that the information and records it withheld under s. 22 consist of information about the victims and other identifiable third parties and is thus "personal information".[49]

[58] I agree with the Ministry that some of the information in question is about identifiable individuals other than the applicant and is therefore their personal information. However, much of the information is about the applicant and is, therefore, his personal information.

Does s. 22(4) apply?

[59] Section 22(4) of FIPPA sets out a number of situations in which disclosure of personal information is not an unreasonable invasion of third-party privacy. The Ministry argued that none of the provisions in s. 22(4) applies in this case.[50] There is no indication in the material before me that s. 22(4) has any relevance in this case. I find that it does not apply.

---

[47] 2015 BCIPC 3 (CanLII), at para. 58.
[48] 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." See Schedule 1 of FIPPA for this definition.
[49] Ministry's initial submission, para. 5.51.
[50] Ministry's initial submission, para. 5.52

*Presumed unreasonable invasion of third-party privac*y – s. 22(3)

[60] The next step is to consider whether disclosure of the information in issue is presumed to be an unreasonable invasion of a third party's personal privacy. The relevant provision is this:

> 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,
>
> …

[61] The Ministry said that some of the information relates to statements made to probation officers while the applicant was being supervised in the community. It argued that the probation officers' community supervision of the applicant was an "investigation" for the purposes of s. 22(3)(b) to supervise the applicant and to determine if he was in violation of his probation. It said that such an investigation could have resulted in a determination that the applicant was breaching his conditions, new charges or variations on his conditions while on probation, which could require bringing an applicant to court.

[62] The Ministry accurately described the information as flowing from supervision of the applicant while he was on bail or probation and from following up on information the Ministry received about him, in connection with various criminal charges. I am satisfied that it was compiled and is identifiable as part of an investigation into a possible violation of law. I therefore find that the presumption against disclosure in s. 22(3)(b) applies to this information.

Relevant circumstances – s. 22(2)

[63] The presumption that disclosure of the withheld information would be an unreasonable invasion of personal privacy can be rebutted. Public bodies must consider all relevant circumstances in determining whether disclosure of personal information is an unreasonable invasion of privacy. The Ministry raised the following relevant circumstances:

> 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
>
> …

> (e) the third party will be exposed unfairly to financial or other harm,
>
> (f) the personal information has been supplied in confidence,
>
> …

[64] Unfair harm – The Ministry said that the records relate to charges against the applicant, a number of which are marked as a "K-file", because the charges relate to "incidents of spousal violence". The Ministry argued that disclosing the information "may also cause the Victims to re-live their experiences or fear for their safety". The Ministry referred to its submission on s. 15(1)(f) in support of its position that s. 22(2)(e) also applies to information that other third parties provided. For all these reasons, the Ministry argued, s. 22(2)(e) weighs in favour of finding that disclosure of the information would be an unreasonable invasion of the privacy of third parties.[51]

[65] Past orders have held that "harm" for the purpose of s. 22(2)(e) consists of "serious mental distress or anguish or harassment".[52] As I discussed above regarding s. 15(1)(f), I recognize that the applicant has been charged with assault on a number of occasions. The Ministry did not however explain how disclosure of the information in question might cause the victims to "re-live their experiences" or "fear for their safety" and thus cause "serious mental distress or anguish or harassment". Moreover, some of the withheld information did not originate with the assault victims but with other individuals. The applicant had good relations with some of these individuals. The information that others provided strikes me as straightforward, even innocuous. It is not clear how these individuals might suffer "serious mental distress or anguish" if the information were disclosed and the Ministry did not explain how this might be so.

[66] I also note that the Ministry has already disclosed some information that BC Corrections staff provided that describes recent hostile, argumentative and rude behaviour by the applicant.[53] There is no evidence that disclosure of this information has exposed these employees to any harm for the purposes of s. 22(2)(e).

[67] The Ministry's arguments as to the possible reactions of the victims or others and the possible behaviour of the applicant are speculative, in my view. The Ministry has not persuaded me that third parties would be exposed to harm on disclosure of the information in question, still less how such exposure would be "unfair". I find that s. 22(2)(e) does not apply here.

---

[51] Ministry's submission, paras. 5.59-5.63.
[52] See for example, Order F12-14, 2012 BCIPC 12, at para. 46, and Order 01-37, 2001 CanLII 21591 (BC IPC), at para. 42.
[53] See, for example, entry on p. 9 dated 2013.02.21 at 12:35:50; entry on p. 10 dated 2013.05.15 at 14:43:35.

[68] Supply in confidence – The Ministry said that the information in question was supplied in confidence, either by the victims or through others. It added that the BC Corrections staff treat such information as confidential, although they may share it with Crown counsel to assist Crown counsel in determining whether an individual has breached bail or probation conditions.[54]

[69] I accept that the information in question was supplied in confidence and I find that s. 22(2)(f) therefore applies to it. This factor favours withholding the information in question.

[70] Applicant's awareness of personal information – Previous orders have found that a relevant circumstance under s. 22(2) is the fact that an applicant is aware of the personal information in issue. It may or may not favour disclosure, depending on the case.[55] The Ministry did not address this issue.

[71] The Ministry explained, on an *in camera* basis, how it withheld, under s. 22(1), some information relating to the Ministry's contact with another body.[56] The already-disclosed information shows that the applicant is aware of this contact and its purpose.[57] Moreover, much of the information concerned is, in my view, as much about the applicant as it is about the others mentioned. Other information is routine and administrative in character and, in my view, raises no privacy concerns. The applicant's awareness of this particular information, together with its administrative character, favours its disclosure.

Is the presumption rebutted?

[72] I find that the applicant's awareness of some of the information weighs in favour of its disclosure and outweighs the s. 22(2)(f) factor. Section 22(2)(e) does not apply to this information. In the case of this information, I find that the presumption in s. 22(3)(b) has been rebutted and that s. 22(1) does not apply to this information.[58]

[73] As for the remaining information, I find that the circumstance in s. 22(2)(e) does not apply. However, I also find the relevant circumstance in s. 22(2)(f) weighs in favour of withholding the personal information that I found above is subject to the presumed unreasonable invasion of personal privacy under s. 22(3)(b). I find that the presumption in s. 22(3)(b) has not been rebutted and that s. 22(1) applies to this information.

---

[54] Clarke affidavit, paras. 19-23.
[55] See, for example, Order 03-24, 2005 CanLII 11964 (BC IPC), and Order F10-41, 2010 BCIPC 61 (CanLII).
[56] Clarke affidavit para. 23, regarding the following: p. 4; entry on pp. 7-8 dated 2013.02.04 at 11:43:30; entry on pp. 8-9 dated 2013.02.21 at 10:05:01; p. 117.
[57] See p. 8.
[58] Page 4; entry on pp. 7-8 dated 2013.02.04 at 11:43:30; entry on pp. 8-9 dated 2013.02.21 at 10:05:01; p. 117. The Ministry did not apply any other exceptions to this information.

Is it reasonable to sever under s. 4(2)?

[74] I noted above that much of the withheld information is the applicant's personal information. Section 4(2) of FIPPA states that, where it is reasonable to sever excepted information from a record, an applicant has the right of access to the remainder. Regarding the information to which I found that s. 22(1) applies, I will now consider whether it is reasonable to sever the third-party personal information from the records in dispute and disclose the applicant's personal information to him.

[75] A number of orders have considered the issue of joint or "inextricably intertwined" personal information of two or more individuals. They have generally found that it is not reasonable to separate an applicant's personal information from a third party's personal information in such cases and that disclosing the joint personal information would be an unreasonable invasion of third-party privacy.[59]

[76] My review of the records reveals that the applicant's personal information is, for the most part, "inextricably intertwined" with third-party personal information. In these cases, it would not, in my view, be possible to disclose the applicant's own personal information to him without also disclosing the third-party personal information. I noted above that disclosure of the third-party personal information to the applicant would be an unreasonable invasion of third-party privacy. Where the applicant's personal information is intertwined with that of third parties, I find that it would not be reasonable to sever the third-party personal information from the record in dispute and disclose the remainder to the applicant.

Summary under s. 22(5)

[77] Under s. 22(5)(a) of FIPPA, a public body must give an applicant a summary of the applicant's personal information, where it was provided in confidence, unless the summary cannot be prepared without revealing the identity of a third party who provided the information in confidence. The Ministry did not address this issue.

[78] I found above that the personal information about the applicant, to which s. 22(1) applies, was supplied in confidence by third parties. However, because a number of third parties provided the information and it is broadly similar in character, I consider that it would be possible to give the applicant a summary of his own personal information without revealing the identities of those who supplied the information in confidence. My order below reflects this finding.

---

[59] See, for example, Order F14-10, 2001 CanLII 21561 (BC IPC), Order F08-02, 2008 CanLII 1645 (BC IPC), and Order 01-07, 2001 CanLII 21561 (BC IPC).

Conclusion on s. 22(1)

[79] I found above that the personal information was compiled and is identifiable as part of an investigation into a possible violation of law, so its disclosure is presumed to be an unreasonable invasion on personal privacy under s. 22(3)(b).

[80] After considering all relevant factors, I found that the presumption had not been rebutted with respect to most of the personal information. However, I found it was rebutted for the personal information that the applicant already knows.

[81] I also found that it is not reasonable to sever the third-party personal information from the record in dispute in order to disclose only the applicant's personal information. I also found that it is possible to prepare a summary of the applicant's personal information under s. 22(5)(a) of FIPPA.

CONCLUSION

[82] For reasons given above, I make the following orders:

1. Under s. 58(2)(a) of FIPPA,
   (a) I require the Ministry to give the applicant access to the information it withheld under s. 22(1), as follows: page 4; entry on pages 7-8 dated 2013.02.04 at 11:43:30; entry on pages 8-9 dated 2013.02.21 at 10:05:01; page 117.
   (b) I require the Ministry to give the applicant access to the information it withheld under s. 15(1)(l).
   (c) subject to paras. 3 and 4 below, I require the Ministry to give the applicant access to the information withheld under s. 15(1)(f).
2. Under s. 58(2)(b) of FIPPA, I confirm that the Ministry is authorized to withhold information as follows:
   (a) under s. 15(1)(g), the following withheld information: page 128, middle entries; page 133, bottom entry; page 134, bottom entry; page 135, third entry; page 149, only entry; last seven lines of the withheld passage on page 150; all of pages 162, 164-180.
   (b) under s. 16(1)(b), the following withheld information: page 7, middle entry; all of pages 157-161.
3. Under s. 58(2)(c), subject to para. 4 below, I require the Ministry to refuse the applicant access to the information it withheld under s. 22(1).

4. Under s. 58(3)(a), I require the Ministry to perform its duty under s. 22(5) to give the applicant a summary of his personal information.

5. As a condition under s. 58(4), I require the Ministry to provide me with the summary required under paragraph 4 above, for my approval, within 15 days of the date of this order, that is, on or before January 18, 2016.

6. The Ministry must give the applicant access to the information noted under paragraphs 1(a) and (b) above and the summary required under paragraph 4 above, within 30 days of the date of this order, that is, on or before February 9, 2016. The Ministry must concurrently copy the OIPC Registrar of Inquiries on its cover letter to the applicant, together with a copy of the records and summary.

December 23, 2015

ORIGINAL SIGNED BY

Celia Francis, Adjudicator

OIPC File No.: F14-57121