OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

Order F25-42

MINISTRY OF PUBLIC SAFETY AND SOLICITOR GENERAL

Carol Pakkala
Adjudicator

June 11, 2025

CanLII Cite: 2025 BCIPC 50
Quicklaw Cite: [2025] B.C.I.P.C.D. No. 50

Summary: An applicant requested, under the *Freedom of Information and Protection of Privacy Act* (FIPPA), access to records from the Ministry of Public Safety and Solicitor General (Ministry). The Ministry provided some responsive records but withheld information from them, citing various sections of FIPPA. The adjudicator found that s. 15(1)(f) (disclosure harmful to law enforcement) applied to the record withheld in its entirety. The adjudicator further found that s. 22(1) (disclosure would unreasonably invade a third party's privacy) authorized the Ministry to withhold some, but not all the information in the other records. The adjudicator ordered the Ministry to disclose to the applicant the information it was not required to withhold.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, RSBC 1996 c 165, ss. 4(2), 15(1)(f), 15(1)(l), 15(2)(c), 19(1)(a), 22(1), 22(2), 22(3)(b), 22(3)(d), 22(4).

INTRODUCTION

[1] The applicant was assaulted by another inmate while in custody at the Surrey Pretrial Services Centre (Centre). The Centre is operated by the Ministry of Public Safety and Solicitor General (Ministry). The applicant requested, under the *Freedom of Information and Protection of Privacy Act* (FIPPA),[1] access to the video (the Video) capturing the assault, pictures of his injuries, and client logs (Logs).

[2] In response to the applicant's access request, the Ministry disclosed the pictures but withheld the entire Video under ss. 15(1) (disclosure harmful to law enforcement), 15(2) (disclosure harmful to proper custody or supervision), 19(1) (disclosure harmful to individual safety), and 22(1) (disclosure would

[1] From this point forward, unless otherwise specified, whenever I refer to section numbers, I am referring to sections of FIPPA.

unreasonably invade a third party's privacy). The Ministry also said it did not have the technological capability to sever the Video other than by removing entire sections of it, so the Video cannot be reasonably be severed in accordance with s. 4(2). The Ministry provided the applicant with a copy of the requested Logs but withheld some information from them under ss.15(1)(f), 15(1)(l), and 22(1).

[3] The applicant requested that the Office of the Information and Privacy Commissioner (OIPC) review the Ministry's decision. The OIPC's investigation and mediation process did not resolve the issues, and the matter proceeded to this inquiry. Both parties provided written submissions and evidence. The Ministry received permission from the OIPC to submit some information *in camera*.

PRELIMINARY MATTERS

Matters outside the scope of FIPPA

[4] The applicant's supporting documentation is extensive and addresses allegations regarding events other than the assault captured in the Video. While I have reviewed this documentation and appreciate how important it is to the applicant that he be heard on these matters, they are outside of my jurisdiction. My authority is limited to deciding whether the Ministry correctly applied FIPPA to the records responsive to his access request.

[5] The applicant does not directly address any of the FIPPA issues in his lengthy submission. For this reason, I make very few references to the applicant's submission in this order.

ISSUES AND BURDEN OF PROOF

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

1. The Ministry is authorized to refuse to disclose the information at issue under ss. 15(1)(f), 15(1)(l), 15(2)(c), or 19(1)(a);

2. The Ministry is required to refuse to disclose the information at issue under s. 22(1); and

3. The Ministry has complied with s. 4(2).

[7] Under s. 57(1) of FIPPA, the Ministry has the burden of proving that disclosure of the information at issue would be harmful under ss. 15(1)(f), 15(1)(l), 15(2)(c), and 19(1)(a).

[8] Under s. 57(2), the applicant has the burden of proving that disclosure of personal information would not be an unreasonable invasion of third party personal privacy under s. 22. However, it is up to the Ministry to establish that the information is personal information.[2]

[9] Past orders establish that when it comes to s. 4(2), the burden is on the Ministry to show that the information cannot reasonably be severed from the record.[3]

DISCUSSION

Background[4]

[10] The Ministry is responsible for the operations of British Columbia's correctional facilities, including the Centre. The applicant was assaulted by another inmate while in custody at the Centre. A surveillance camera captured this assault on the Video. Corrections staff used the Video for the purpose of reviewing and investigating the assault.

Information at issue

[11] The responsive records at issue in this case are the Video and the Logs. The Ministry provided both for my review.

[12] The Video, which is 2 minutes and 1 second long, captures the assault on the applicant.[5]

[13] The Logs document certain events that occurred in relation to the applicant while he was in custody at the Centre. The information withheld from the Logs includes the numerical body scanner level used to scan the applicant for contraband; the address and phone number of an individual to whom the applicant sent mail; the name and inmate number of the inmate who assaulted the applicant; and an Internal Directory and Authentication Service (IDIR) username assigned to a corrections employee.

[14] The Ministry is no longer refusing access to the numerical body scanner level,[6] so I consider that information is no longer at issue.

---

[2] Order 03-41, 2003 CanLII 49220 (BC IPC) at paras 9-11.
[3] Order 03-13, 2003 CanLII 49182 (BC IPC) at para 7.
[4] The information in this section is drawn from the parties' submissions and evidence.
[5] Affidavit of Assistant Deputy Warden at para 12.
[6] Ministry's initial submissions at para 20.

Disclosure harmful to law enforcement – s. 15

[15] Section 15 allows a public body to refuse to disclose information to an applicant if its disclosure could reasonably be expected to be harmful to law enforcement. The phrase "could reasonably be expected to be harmful" means a reasonable expectation of probable harm. This standard is a middle ground between that which is probable and that which is merely possible.[7] Further, there must be a clear and direct connection between the disclosure of specific information and the harm that is alleged.[8]

[16] The Ministry's position is that ss. 15(1)(f), 15(1)(l), and 15(2)(c) apply to the entire Video and to some of the information in the Logs. Those provisions state:

> 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,
> …
>
> (l) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.
>
> (2) The head of a public body may refuse to disclose information to an applicant if the information
> …
>
> (c) is about the history, supervision or release of a person who is in custody or under supervision and the disclosure could reasonably be expected to harm the proper custody or supervision of that person.

Safety of law enforcement officer – s. 15(1)(f)

[17] Section 15(1)(f) provides that a public body may refuse to disclose information whose disclosure could reasonably be expected to endanger the life or physical safety of a law enforcement officer or any other person.

---

[7] *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner),* 2014 SCC 31 at para 54.
[8] Order F17-15, 2007 CanLII 35476 (BCIPC) at para 17.

Parties' positions – s. 15(1)(f)

[18] The Ministry says that disclosure of the Video and the IDIR username in the Logs could reasonably be expected to endanger the life or physical safety of a law enforcement officer or any other person.[9]

[19] The Ministry says the Video provides valuable information to inmates about where and how to engage in harmful conduct within the Centre. The Ministry says such knowledge increases the risk of inmates engaging in conduct harmful to life or physical safety.[10] For the IDIR username, the Ministry says its disclosure would compromise the safety of corrections staff because it would identify the individual that entered information into the Logs.

[20] To support its position on s. 15(1)(f), the Ministry relies on the Video itself which it says is highly persuasive evidence that supports the Ministry's decision to refuse access.[11] The Ministry also relies on the affidavit of the Centre's Assistant Deputy Warden (Warden) who deposes:

- The Video provides substantive sensitive information, including camera location and angles, revealing areas covered by video surveillance and areas shielded from view in whole or in part.
- The Video reveals information about corrections staff including their location and number in the area, response time, and information about how they coordinate and communicate when responding to violent incidents.[12]
- Disclosure of the Video to the applicant is disclosure to the world such that it could be posted on social media and shared widely. Inmates across BC could study and learn from it and use that knowledge against corrections staff.[13]
- It is the Ministry's practice to withhold from inmates the names of correctional officers who report certain allegations.[14]

[21] Additionally, the Warden provides further particulars, received by the OIPC *in camera*, about the events depicted in the Video.

[22] The applicant does not comment on the expectation of harm in relation to disclosure of the Video or the IDIR username or respond to the Ministry's submission and evidence about why it refused access under s. 15(1)(f). The applicant does comment on the safety of himself and of other inmates in relation

[9] Ministry's initial submission at para 30.
[10] Ministry's initial submission at para 35.
[11] Ministry's initial submission at para 20.
[12] Assistant Deputy Warden's affidavit at para 18.
[13] Assistant Deputy Warden's affidavit at para 20-21.
[14] Assistant Deputy Warden's affidavit at para 26.

to their treatment by the correctional officers. The applicant says the Video should be disclosed to minimize the misconduct of the correctional officers.[15]

Analysis - s. 15(1)(f)

[23] For the reasons that follow, I find disclosure of the Video, but not the IDIR username, could reasonably be expected to cause the type of harm s. 15(1)(f) is intended to prevent.[16] In making this finding, consistent with past orders, I accept that disclosure to the applicant must be treated as disclosure to the world as there would be nothing to prevent him disclosing the information to others.[17]

[24] For the Video, I give weight to the *in camera* portion of the Warden's evidence because of my own review of the Video evidence. My review of this evidence convinces me that disclosure of the Video poses a risk to the physical safety of inmates and correctional staff.

[25] In my view, the Video provides valuable information to inmates about where and how to engage in harmful conduct within the Centre. I can see that it provides substantive information about camera location and angles, revealing areas covered by video surveillance and areas shielded from view, in whole or in part. Physical harm to the applicant was captured by these cameras and in my view, there is a reasonable expectation of such harm reoccurring if the Video were disclosed.

[26] I find therefore that disclosure of the Video could reasonably be expected to endanger the physical safety of both correctional staff and inmates. I further find the evidence establishes a clear and direct connection between disclosure of the Video and this reasonable expectation of harm under s. 15(1)(f). I cannot say more without revealing the *in camera* evidence or the information at issue.

[27] For the IDIR username, I cannot see how disclosure of the name of a correctional officer who entered information into the Logs could reasonably be expected to endanger their life or physical safety. Correctional officers are tasked with monitoring the activities of the inmates. Entering information into the Logs is part of their duties. In other words, the correctional officer was doing his or her job.

[28] I am not convinced that disclosing the fact of simply doing ones' job, even in the correctional setting, could reasonably be expected to endanger ones' life or physical safety. The Ministry also withheld the IDIR username under ss. 15(1)(l) and 22(1) so I consider this information further below.

---

[15] Applicant's submission at p. 2-3.
[16] I am satisfied correctional officers are "law enforcement" officers for the purposes of s. 15(1)(f).
[17] Order F21-65, 2021 BCIPC 76 (CanLII) at para 58 and Order 03-35, 2003 CanLII 49214 (BC IPC) at para 31.

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

[29] Section 15(1)(l) provides that a public body may refuse to disclose information whose disclosure 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.

Parties' positions – s. 15(1)(l)

[30] The Ministry says that disclosure of the IDIR username could reasonably be expected to harm the security of the government's computer system. The Ministry says disclosure of the IDIR username creates a real risk of unauthorized individuals using it to potentially access the government's computer system which it says can and has resulted in substantive harms to government.[18]

[31] To support its position, the Ministry relies on the affidavit of the Chief Information Security Officer for the Province of British Columbia (Officer) who deposes the following about IDIR usernames:

- They are not publicly available.
- The government treats them as confidential for security reasons as the username forms half the credentials required to authenticate an individual's identity.
- They are harder to guess because they are not all the same length and do not follow a standard combination of letters from someone's name. Instead, they are a unique combination of letters derived from a person's first and last name.[19]

[32] The Officer believes that disclosing IDIR usernames would increase the risk of unauthorized access to the government's computer system. She says that "it is a fundamental and widely accepted principle of system security that the less system information an attacker has about a system, the harder it will be for them to attack or otherwise compromise the privacy and security of a system and its data."[20]

[33] The Officer explains that attackers could use IDIR usernames for the appearance of legitimacy or credentials that they do not have, thereby facilitating indirect attacks, such as phishing.[21]

---

[18] Ministry's initial submission at para 51.
[19] A/ Chief Information Security Officer for the Province of British Columbia (Officer)'s affidavit at paras 12-13.
[20] Officer's affidavit at para 17.
[21] Officer's affidavit at paras 35-36.

[34] The Officer says hackers could also directly target and attack the government's computer system if they had an IDIR username. She says guessing both the IDIR username and the password is more difficult than guessing the password alone. The Officer believes users often rely on the same passwords for different applications which makes guessing passwords easier and increases the necessity to keep usernames secure.[22]

[35] The applicant did not respond directly to the Ministry's submissions and evidence regarding the IDIR information and s. 15(1)(l).

Analysis - s. 15(1)(l)

[36] Section 15(1)(l) explicitly refers to harm to security of a "computer system". I am satisfied that the government computer network is a "system" for the purposes of s. 15(1)(l). Previous OIPC orders have reached the same conclusion.[23] However, for the reasons to follow, I am not satisfied that the disclosure of the Ministry IDIR username at issue here could reasonably be expected to threaten the security of the government's computer system.

[37] The alleged harm at issue here is the unauthorized access of the province's computer system by hackers. The Ministry's position is that disclosing the IDIR username increases the risk of someone gaining that unauthorized access. This proposition is clearly speculative. The Ministry's evidence to support this position is about government-wide computer systems and the general tactics of hackers.

[38] In my view, it is not reasonable to assume there are no security measures or protocols in place to detect or prevent such unauthorized access. It is not credible to conclude that the government's computer systems are that "fragile".[24]

[39] For the reasons given above, I find the Ministry has not provided sufficient explanation or evidence to demonstrate that disclosure will result in a risk of harm that is well beyond the merely possible or speculative or that there is a direct connection between the disclosure of the information at issue and the alleged threat to the government's computer system. As a result, I conclude the Ministry is not authorized to withhold the information at issue under s. 15(1)(l).

[40] My conclusions and findings are consistent with previous OIPC orders that have found s. 15(1)(l) does not apply to IDIR usernames[25] and comparable

---

[22] Officer's affidavit at paras 30-33.
[23] Order F21-35, 2021 BCIPC 43 (CanLII) at para 89; Order F15-47, 2015 BCIPC 78 (CanLII) at para 18; and Order F18-38, 2018 BCIPC 41 (CanLII) at paras 55-59
[24] For similar analysis see: Order 23-100, 2023 BCIPC 116 (CanLII) at para 49; Order F21-35, 2021 BCIPC 43 (CanLII) at para 93; and Order F10-39, 2010 CanLII 77325 (BC IPC) at para 17.
[25] Order F21-35, 2021 BCIPC 43 (CanLII).

information (i.e., user login IDs).[26] The public bodies in those cases made similar assertions and arguments in their submissions and affidavit evidence about the alleged harm.

[41] I find that s. 15(1)(l) does not apply to the IDIR username.

Harm to proper custody or supervision – s. 15(2)(c)

[42] Section 15(2)(c) provides that a public body may refuse to disclose information that is about the history, supervision, or release of a person who is in custody or under supervision where disclosure could reasonably be expected to harm the proper custody or supervision or that person. The Ministry applied s. 15(2)(c) to the Video. Given my findings under s. 15(1)(f), I need not consider whether s. 15(2)(c) also applies.

Disclosure harmful to safety – s. 19

[43] Section 19(1)(a) allows a public body to refuse to disclose information, including personal information about an applicant, if the disclosure could reasonably be expected to threaten anyone else's safety or mental or physical health. The Ministry says that s. 19(1)(a) applies to the Video.

[44] Since the Video captures the assault on the applicant, it includes his personal information. Given my findings under s. 15(1)(f) though, I need not consider whether s. 19(1) also applies.

Disclosure harmful to third party personal privacy – s. 22

[45] Section 22 requires a public body to refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.[27] This provision of FIPPA is mandatory, meaning a public body has no discretion and is required by law to refuse to disclose this information. Previous orders have considered the proper analytical approach to the application of s. 22 which I apply below.[28]

[46] The Ministry applied s. 22 to the Video. Given my findings under s. 15(1)(f), I need not consider whether s. 22 also applies to the Video. The Ministry also applied s. 22 to information in the Logs. This information includes the name and inmate number of the individual who assaulted the applicant, the

[26] Order F10-39, 2010 CanLII 77325 (BC IPC); Order F15-72, 2015 BCIPC 78; Order F14-12, 2014 BCIPC 15 (CanLII); Order F10-25, 2010 BCIPC 36 (CanLII).
[27] Schedule 1 of FIPPA defines a "third party" to mean "any person, group of persons or organization other than (a) the person who made the request, or (b) a public body."
[28] Order F15-03, 2015 BCIPC 3 (CanLII) at para. 58 sets out a summary of the steps in a s. 22 analysis which I follow here.

address and phone number of an individual to whom the applicant sent mail, and the IDIR username.

[47] The Ministry's submissions on s. 22 are primarily about the Video. The applicant does not say anything about the application of s. 22. While I have read the submissions of both parties in their entirety, I will not refer to them further in the s. 22 analysis except as they may relate to the withheld information.

Personal information

[48] Section 22(1) only applies to personal information, so the first step in a s. 22 analysis is to decide if the information in dispute is personal information.

[49] FIPPA defines personal information 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."[29] Whether information is "contact information" depends upon the context in which it appears.[30]

[50] I will first consider whether the information in the records in dispute is about identifiable individuals. I will then consider whether any of the information that I find is about identifiable individuals is contact information.

Analysis - personal information

[51] The information withheld under s. 22(1) includes the IDIR username, a name and inmate number, and an address and phone number. I find that all of this information is about identifiable individuals. It either directly identifies individuals by name or is reasonably attributable to a particular individual, on its own or when combined with other available sources of information.

[52] From the context provided by the records, it does not appear to me that the address and phone number were provided for that individual to be contacted at a place of business, so it is not contact information.

[53] I find that all the information severed under s. 22 is personal information.

[29] FIPPA, Schedule 1.
[30] Order F20-13, 2020 BCIPC 15 (CanLII) at para 42.

Not an unreasonable invasion of third party personal privacy - s. 22(4)

[54] The next step in the s. 22 analysis is to determine whether the personal information falls into any of the categories set out in s. 22(4) and is, therefore, not an unreasonable invasion of a third party's personal privacy. I considered all the provisions in s. 22(4) and find that none apply.

Presumed unreasonable invasion of third party personal privacy - s. 22(3)

[55] The third step in the s. 22 analysis is to determine whether any presumptions set out in s. 22(3) apply. Section 22(3) sets out circumstances where disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy.

[56] In my view, the only provision that has some relevance to the information at issue is s. 22(3)(d).

[57] The relevant portions of s. 22(3) say:

> A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if
> …
>
> (d) the personal information relates to employment, occupational or educational history,
>
> …

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

[58] The IDIR username is a unique personal identifier within the government's computer system. Previous OIPC orders have found that personal identifiers for an employee may form part of their employment history under s. 22(3)(d).[31] I agree.

[59] I conclude the presumption under s. 22(3)(d) applies to the IDIR username since it is assigned to the correctional officer and used by them as part of their employment. Therefore, I conclude this personal identifier is a part of their employment history and its disclosure is presumed to be an unreasonable invasion of third party personal privacy under s. 22(3)(d).

[31] Order F21-35, 2021 BCIPC 43 (CanLII) at para 189, Order F14-41, 2014 BCIPC 44 (CanLII) at para 46; Order F15-17, 2015 BCIPC 18 (CanLII) at para 37 and Order 03-21, 2003 CanLII 49195 at paras 25-26.

[60] In summary, I find that ss. 22(3)(b), and (d) apply to some of the personal information at issue.

Relevant circumstances – s. 22(2)

[61] The final step in the s. 22 analysis is to consider the impact of disclosure of the personal information while considering all relevant circumstances, including (but not limited to) those set out in s. 22(2). It is at this step that any applicable s. 22(3) presumptions may be rebutted.

[62] I find that there are no relevant circumstances that weigh in favour of disclosure of the inmate's name and number or the IDIR username. For the address and phone number of the third party, the Ministry says, and I can see in the records, that this information pertains to an individual to whom the applicant sent mail. The applicant's knowledge is a relevant circumstance, so I consider it further below.

Applicant's knowledge

[63] Past orders have held that the fact that an applicant already knows the third party personal information in dispute is a relevant circumstance that may weigh in favour of disclosure.[32] Such knowledge is often given limited weight because the information known to an applicant is not known to the world at large.

[64] The Ministry says it withheld the address and phone number despite the applicant's knowledge because disclosure to the applicant is disclosure to the world.[33] In my view, there is no real potential for an invasion of this person's personal privacy arising from disclosure of the address and phone number. If the applicant wanted to disclose this information, he could already do so. For that reason, I conclude the applicant's knowledge weighs in favour of disclosure.

Conclusion, s. 22(1)

[65] I found that all the information withheld by the Ministry under s. 22(1) is personal information and that s. 22(4) does not apply. I also found that a presumption of an unreasonable invasion of third party personal privacy under ss. 22(3)(b) and (d) applies to name and inmate number of the individual who assaulted the applicant and to the IDIR username.

[66] After considering the relevant circumstances under s. 22(2) (both listed and unlisted), I conclude that disclosing the personal information, except for the address and phone number, would be an unreasonable invasion of a third party's

[32] Order F17-02, 2017 BCIPC 2 (CanLII) at paras 28-30, Order 03-24, 2005 BCIPC 11964 (CanLII) at para 36, and Order F15-14, 2015 BCIPC 14 (CanLII) at paras 72-74.
[33] Ministry's initial submission at para 105.

personal privacy. The Ministry must withhold the name and inmate number and the IDIR username under s. 22(1).

Reasonable severing – s. 4(2)

[67] Section 4(2) provides that an applicant's right of access to a record does not extend to information that is subject to a disclosure exception, but if that excepted information can reasonably be severed from a record, the applicant has a right of access to the remainder of the record.

[68] The Ministry argued that the entirety of the Video is subject to one or more access exceptions, that severing certain information in the Video by blurring it out would render the remainder incomprehensible, unintelligible and meaningless, so the Video cannot reasonably be severed and there is no "remainder of the record" that the Applicant has a right of access to under s. 4(2).[34]

[69] Given my finding that the entire Video may be withheld under s. 15(1)(f), I need not decide anything about s. 4(2).

CONCLUSION

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

1. The Ministry is authorized to refuse to disclose all of the Video under s. 15(1)(f).

2. Subject to item 3 below, I require the Ministry to refuse access to the personal information at issue under s. 22(1).

3. The Ministry is not required to refuse to disclose the address and phone number on pages 1 and 3 of the records.

4. I require the Ministry to give the applicant access to the information that it is not required to withhold as described in item 3 above.

5. The Ministry must concurrently provide the OIPC's registrar of inquiries with a copy of its cover letter and the records it provides to the applicant in compliance with item 3 above.

[34] Ministry's initial submission at paras 110-114.

[71] Pursuant to s. 59(1) of FIPPA, the Ministry is required to comply with this order by July 24, 2025.

June 11, 2025

ORIGINAL SIGNED BY

Carol Pakkala, Adjudicator

OIPC File No.: F23-92697