ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2021-34

September 1, 2021

JUSTICE AND SOLICITOR GENERAL

Case File Number 005482

Office URL: www.oipc.ab.ca

Summary: An individual made an access request to Justice and Solicitor General (the Public Body) under the *Freedom of Information and Protection of Privacy Act* (FOIP Act) for all records containing information about him, his two children and his spouse.

The Public Body provided responsive records to the Applicant, with information withheld under sections 17(1), 18(1), 20(1) and 21(1). Some records were withheld in their entirety under section 4(1)(a) and a video was withheld in its entirety under section 17(1).

The Applicant requested an inquiry into the Public Body's response, specifically regarding the Public Body's application of sections 18(1), 20(1) and 21(1) of the Act.

The Adjudicator determined that the Public Body properly applied section 18(1)(a) to the information in the records. The Adjudicator also determined that section 18(1)(a) applied to information that had been withheld under section 21(1)(b) but that was substantially similar to other information withheld under section 18(1)(a) and for which the Public Body's reasons for withholding from the Applicant were similar.

The Adjudicator found that the Public Body properly applied section 20(1)(m) to information in the records.

The Adjudicator decided to retain jurisdiction regarding the Public Body's application of section 21(1)(b), pending the appeal of *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2021 ABQB 304.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 18. 20, 21, 72.

Authorities Cited: AB: Orders 99-018, F2002-024, F2004-018, F2004-029, F2008-017, F2008-027, F2009-009, F2009-027, F2009-038, F2010-036, F2013-51, F2017-60, F2019-09, F2020-08, F2020-17, F2020-22, H2002-001

Cases Cited: *Canada (Information Commissioner) v. Canada (Prime Minister)*, 1992 CanLII 2414 (FC), [1992] F.C.J. No. 1054, Edmonton Police Service v. Alberta (Information and Privacy Commissioner), 2012 ABQB 595, *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2020 ABQB 10, (CanLII) *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2021 ABQB 304, *Ontario (Public Safety and Security) v. Criminal Lawyers' Association,* 2010 SCC 23 (CanLII), *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31, 2021 ABPC 41

I. BACKGROUND

[para 1] An individual made an access request to Justice and Solicitor General (the Public Body) under the *Freedom of Information and Protection of Privacy Act* (FOIP Act) for the following:

> I would like to request any all emails, to and from; texts, to and from; audio and video, written correspondence of any kind, documents of any kind, briefing notes, files of any kind, written material of any kind, letters, drawings, photos, faxes, reports of any kind, reporting; consultations, interpretations of any kind, reviews, written summaries of any kind, analyses of any kind, assessments of any kind; notes of any kind, minutes of any and all meetings (in person and electronic / video / teleconference), communication of any kind in any format of the following individuals […] involving myself […], and/or my two children, […] and /or my wife […] between the time period of August 2, 2014 to the present.

[para 2] The Public Body located 94 pages of responsive records, as well as a responsive video. The Public Body withheld some records in their entirety under section 4(1)(a); it also withheld the video in its entirety under section 17(1). The Public Body provided 62 pages of records to the Applicant with some information withheld under sections 17(1), 18(1), 20(1) and 21(1).

[para 3] The Applicant requested a review of the Public Body's response. The Commissioner authorized mediation to attempt to settle the matter. Following the mediation, the Applicant requested an inquiry into the Public Body's application of section 18(1), 20(1), and 21(1) to information in the records.

[para 4] As the inquiry does not encompass the application of sections 4(1) or 17(1), the records withheld under those provisions are not at issue, including the video.

II. RECORDS AT ISSUE

[para 5] The records at issue consist of the withheld portion of the records provided to the Applicant on April 28, 2016.

III. ISSUES

[para 6] The issues as set out in the Notice of Inquiry, dated February 16, 2021, are as follows:

1. Did the Public Body properly apply section 18 of the Act (disclosure harmful to individual or public safety) to the information it severed from the records under this provision?

2. Did the Public Body properly apply section 20(1)(m) of the Act (disclosure harmful to law enforcement) to the information it severed from the records under this provision?

3. Did the Public Body properly apply section 21(1) of the Act (disclosure harmful to intergovernmental relations) to the information it severed from the records under this provision?

IV. DISCUSSION OF ISSUES

Preliminary discussion – submissions from the parties

[para 7] A significant portion of the Public Body's submissions in this inquiry, especially the submissions relating to the application of section 18(1)(a), have been accepted *in camera*. This is because those submissions included information the Public Body would have been permitted to withhold under the FOIP Act, or that revealed withheld information in the records. Section 69(3) of the Act contemplates *in camera* submissions being made during the inquiry process. It states:

> *69(3) The person who asked for the review, the head of the public body concerned and any other person given a copy of the request for the review must be given an opportunity to make representations to the Commissioner during the inquiry, but no one is entitled to be present during, to have access to or to comment on representations made to the Commissioner by another person.*

[para 8] The Applicant had limited ability to provide a response to the Public Body's arguments made *in camera*.

[para 9] In his initial submission, the Applicant states:

> In relation to the above noted Inquiry by the OIPC of Alberta, the Applicant relies on the attachments to the Notice of Inquiry (dated 09/10/2017); along with the references (as noted in the initial request for Inquiry, dated 09/10/2017) to other formal complaints that were previously made to the OIPC of Alberta (regarding the Calgary Police Service ('CPS') and certain named employees thereof, submitted in July, August and September 2017). Please note that the OIPC of Alberta has such documentation in its possession. Hence, for simplicity, it will not be repeated in this instance.

[para 10] The Notice of Inquiry clearly informs the parties that the only information before me, other than the submissions to be made by the parties, is the Applicant's request for review and request for inquiry (along with attachments).

[para 11] By letter dated May 28, 2021, I reminded the Applicant that only his request for review, request for inquiry, an initial submission were before me. I informed him that other documents, including documents he had provided to this Office in relation to other files, were not before me. I invited the Applicant to provide any additional documents he wanted me to consider with his rebuttal submission.

[para 12] In his rebuttal submission, the Applicant again refers to documents previously provided to this Office in relation to other files; however, he did not provide these documents with his submission. Without the documents, I do not know what they contain, what type of documents they are, who created the documents, or the context of the information the Applicant has referred to being in the documents. Without this information, I cannot give weight to the Applicant's submissions regarding what these documents contain or how they support the Applicant's arguments.

1. Did the Public Body properly apply section 18 of the Act (disclosure harmful to individual or public safety) to the information it severed from the records under this provision?

[para 13] Section 18(1)(a) states:

> *18(1) The head of a public body may refuse to disclose to an applicant information, including personal information about the applicant, if the disclosure could reasonably be expected to*
>
> *(a) threaten anyone else's safety or mental or physical health*
>
> ...

[para 14] In Order H2002-001, former Commissioner Work considered what must be established in order for section 11(1)(a)(ii) of the *Health Information Act*, which is similar to section 18 of the FOIP Act, to be applicable. He reviewed previous Orders of this Office addressing what is necessary to establish a reasonable expectation of harm under section 18 of the FOIP Act and adopted the following approach:

> In Order 2001-010, the Commissioner said there must be evidence of a direct and specific threat to a person, and a specific harm flowing from the disclosure of information or the record. In Order 96-004, the Commissioner said detailed evidence must be provided to

> show the threat and disclosure of the information are connected and there is a probability that the threat will occur if the information is disclosed.

[para 15] This analysis has been followed with respect to section 18(1)(a) of the FOIP Act. In Order F2013-51, the Director of Adjudication reviewed past orders of this office regarding the application of section 18. She summed up those orders as follows (at paras 20-21):

> These cases establish that section 18 of the FOIP Act applies to harm that would result from disclosure of information in the records at issue, but not to harm that would result from factors unrelated to disclosure of information in the records at issue. Further, a public body applying section 18 of the FOIP Act must provide evidence to support its position that harm may reasonably be expected to result from the disclosure of information (as must a custodian applying section 11(1)(a) of the HIA).
>
> Following the approach adopted by the former Commissioner in Order 96-004, and in subsequent cases considering either section 18 of the FOIP Act or section 11 of the HIA, the onus is on the Public Body to provide evidence regarding a threat or harm to the mental or physical health or safety of individuals, to establish that disclosure of the information and the threat are connected, and to prove that there is a reasonable expectation that the threat or harm will take place if the information is disclosed.

[para 16] In Order F2004-029, the adjudicator also stated that "being difficult, challenging, or troublesome, having intense feelings about injustice, being persistent, and to some extent, using offensive language, do not necessarily bring section 18 into play" (at para. 23).

[para 17] I agree with the above analyses. Further, the Supreme Court of Canada has clearly enunciated the test to be used in access-to-information legislation wherever the phrase "could reasonably be expected to" is found (such as in section 18(1)(a)). In *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 (CanLII), the Court stated:

> Given that the statutory tests are expressed in identical language in provincial and federal access to information statutes, it is preferable to have only one further elaboration of that language; *Merck Frosst*, at para. 195:
>
> > I am not persuaded that we should change the way this test has been expressed by the Federal Courts for such an extended period of time. Such a change would also affect other provisions because similar language to that in s. 20(1)(c) is employed in several other exemptions under the Act, including those relating to federal-provincial affairs (s. 14), international affairs and defence (s. 15), law enforcement and investigations (s. 16), safety of individuals (s. 17), and economic interests of Canada (s. 18). In addition, as the respondent points out, the "reasonable expectation of probable harm" test has been followed with respect to a number of similarly worded provincial access to information statutes. Accordingly, the legislative interpretation of this expression is of importance both to the application of many exemptions

> in the federal Act and to similarly worded provisions in various provincial statutes. [Emphasis added.]
>
> 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.

[para 18] The Supreme Court of Canada has made it clear that there is one evidentiary standard to be used wherever the phrase "could reasonably be expected to" appears in access-to-information legislation. There must be a reasonable expectation of probable harm, and the Public Body must provide sufficient evidence to show that the likelihood of any of the above scenarios is "considerably above" a mere possibility.

[para 19] In Order F2017-60, I accepted that the names and contact information of Civil Forfeiture Office (CFO) employees in Justice and Solicitor General could be withheld under section 18(1). The CFO restrains and forfeits property found to be obtained by crime or used to commit a crime.

[para 20] The evidence I considered persuasive in that case included the fact that steps were taken to ensure that these employees do not deal directly with individuals whose property is seized; even contact with service providers is done with a general email address and not an address that identifies the individual employee.

[para 21] In that case, I also accepted that CFO employees deal with individuals accused of, or convicted of, serious offences under the *Criminal Code* or *Controlled Drugs and Substances Act*. I found that this "makes the likelihood of a threat to safety or health higher than it would be in relation to other public body employees that may deal with a very small percentage of such individuals" (at para. 45). I also noted that property confiscated by the CFO may not have been merely the proceeds of crime but also the means by which crimes were committed; this is an additional motive for those individuals to attempt to regain the property by harassing or threatening CFO employees who know the location of the property.

[para 22] I also noted in that case that the finding was fact-specific. I said (at para. 50):

> This finding should be kept to the particular facts of this case. It is not unusual for public body employees to have to deal with difficult, or even violent members of the public, in the normal course of their duties. I do not mean to suggest that the names of those employees also ought to be withheld from the public.

[para 23] In Order F2019-09, I considered a Public Body's application of section 18(1) to withhold a staff directory from an applicant. In that case, the Public Body argued that it has had to implement a communications protocol with respect to certain individuals, who had made abusive or harassing calls to employees of the public body. The protocols included limiting these individuals to a single point of contact with the public body; other employees were not required to take the calls of those individuals.

[para 24] I found that having had to implement a communications protocol does not meet the standard for section 18(1). I said (at para. 51):

> As noted in Orders F2004-029 and F2017-60, it is not unusual for public body employees to deal with difficult, aggressive, harassing, abusive, or even violent individuals. The Public Body has a communications protocol to address these individuals, such that Public Body employees are not required to handle those calls, outside the single point of contact. Absent additional evidence of a specific threat or harm, the fact that some individuals are abusive on the phone is not sufficient to meet the standard required by section 18(1).

[para 25] In Order F2020-08 I again considered whether the business contact information of specific public body employees could be withheld under section 18(1). I found (at paras. 49-52):

> Several employees provided sufficient evidence to meet the test for section 18(1)(a). Evidence included information about past situations in which personal contact information had been used to harass, stalk, and impersonate the employees. To be clear, this harassment etc. amounted to more than unpleasant conversations with members of the public; these circumstances as described to me threatened the safety or security of the employee and/or their families. In these cases, I have accepted that section 18(1)(a) applies to the employees' information in the records at issue, as the disclosure of additional contact information could reasonably be expected to lead to similar harassment etc. as the personal contact information had already been used to perpetrate.
>
> Where an employee has recently had issues with identity theft using their personal contact information, it seems reasonable to expect that disclosing additional contact information, including business contact information, could perpetuate this harm. In other words, a problem already exists and disclosing additional information, even information as innocuous as a job title, work phone number and email, could make the existing problem worse.
>
> In contrast, where no problem exists, it is difficult to see how disclosing business contact information could reasonably be expected to *lead* to identity theft. This is especially true for those employees who have disclosed work-related information online, which a number of the employees making submissions to this inquiry have done. With respect to general phishing scams and phone scams, these occur seemingly regardless of whether the information is on a publicly available directory or not. Without additional information showing that additional information of the employee has already been obtained and used for such purposes, I find the general concerns about phishing and identity theft to be too speculative to meet the standard for section 18(1)(a).

> Many employees expressed concern about an increase in abusive communications if their direct email addresses and phone numbers are disclosed. I rejected that argument in Order F2019-09 (at paras. 43, 49-51) and again at paragraphs 37-38 of this Order. In contrast, where an employee has provided sufficient evidence to show that their personal information has been used to harass the employees, that harassment has amounted to more than unpleasant calls; it has called into question the safety of the employee. I cannot provide more detailed reasons for this finding in my public order, in case those reasons identify the employees who have made these arguments.

[para 26] In this case, the Public Body has made its submissions regarding the application of section 18(1) *in camera*. I cannot reveal the details of those submissions and can only discuss them in general terms. I can say that the Public Body withheld only discrete items of information that serve to identify public body employees. Information pertaining to the Applicant and his interactions with the Public Body has been disclosed to him.

[para 27] The Public Body has provided information about the Applicant's past interactions with the Public Body and other public bodies. Its submissions on the application of section 18(1)(a) to withhold identifying information of public body employees focusses on arguments specific to these interactions. In other words, the Public Body's application of section 18(1)(a) is specific to the Applicant and the particular circumstances of this case.

[para 28] The Applicant's ability to respond to these arguments was limited. In his rebuttal submission, he states:

> Additionally, the Applicant had initially provided the OIPC with records of detailed written threats made towards the Applicant by two (2) female individuals; one (1) being a female CPS police officer and the other being a female employee of the not for profit entity, HomeFront Calgary. Therefore, given the previously obtained explicit emailed statements of various public and charitable employees, the Applicant will again highlight the fact that it is actually the Applicant who needs to be afraid of the CPS and other individuals; rather than other so called individuals/victims that the Public Body and the CPS refer to in the recent rebuttal. Hence, the requested records should be released to the Applicant as there is no reasonable risk to others.

[para 29] As mentioned earlier in this Order, I do not have documents provided by the Applicant to this Office for other files. I invited the Applicant to provide the documents he has referred to, but he did not do so. As such, I do not know what emails the Applicant is referring to, who sent them, or their contents.

[para 30] The Applicant did provide a citation to a decision of the Provincial Court of Alberta (2021 ABPC 41) relating to a charge brought against him by the Crown that he repeatedly communicated with the director of corporate security services within the Public Body, "without lawful excuse and with the intent to harass" this employee (section 372(3) of the *Criminal Code*). I have reviewed this decision.

[para 31] The finding of the Court is that the Crown failed to show, beyond a reasonable doubt, that the repeated communications from the Applicant to this Public Body employee were done with the intent to harass the employee. The Court accepted that the repeated communications were made by the Applicant because he had been seeking the name of the employee's supervisor, and not because the Applicant intended to harass the employee.

[para 32] I understand why the Applicant believes this decision supports his position; however, while he was found not to have intended to harass the employee with repeated communications, this is not determinative for the purposes of section 18(1)(a). The standard under the *Criminal Code* for showing the Applicant committed the act he was charged with is different from the standard for finding that section 18(1)(a) applies. The standard for the applicable provision under the *Criminal Code* is "beyond a reasonable doubt", as stated in the Court decision. In contrast, the standard for applying section 18(1)(a) is on the balance of probabilities. More importantly, under section 18(1)(a), intent is not relevant; specifically, there needn't be an *intent* to present a reasonable expectation of harm.

[para 33] The Applicant has also argued that it is the Public Body, and various employees within the Public Body, who have been harassing him. However, as discussed earlier, the Applicant has not provided me with any documents he states support this allegation.

[para 34] I find that the Public Body's application of section 18(1)(a) is appropriate in this case. The Public Body has provided sufficient evidence to find that disclosing the withheld information could reasonably be expected to threaten safety or mental or physical health of the individuals the information is about.

[para 35] I can also say that my finding in this case is consistent with past Orders of this Office. The Public Body's submissions indicate that the harm alleged is direct and specific, rather than general in nature. The Public Body did not apply this provision to information that reveals the identity of all public body employees; only the identity of a few employees was withheld from the Applicant. Whether the Public Body had to implement a "communications protocol" for the Applicant, to limit his contact with public body employees was not a determinative factor. The behavior discussed by the Public Body amounts to more than dealing with a difficult, challenging, or persistent individual. In this case, it would not be unreasonable for an individual whose information is withheld under section 18(1)(a) to experience a level of alarm if their information were disclosed to the Applicant, that is commensurate with the standard to be met for section 18(1)(a).

[para 36] As in Order F2017-60, this finding is fact-specific.

[para 37] Section 18(1)(a) is a discretionary provision. Given the harms discussed by the Public Body in its submissions, and that I have found these harms to reasonably be

expected to occur, I am satisfied that the Public Body properly exercised its discretion to apply that provision.

2. Did the Public Body properly apply section 20(1)(m) of the Act (disclosure harmful to law enforcement) to the information in the records?

[para 38] The Public Body applied this provision to discrete items of information in the footer of several pages of records that show the "path of the computer system" used to view or print information.

[para 39] Section 20(1)(m) states:

> *20(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to*
>
> *...*
>
> *(m) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system,*
>
> *...*

[para 40] Section 20(1)(m) permits the Public Body to withhold information if the disclosure of that information could reasonably be expected to harm the security of any property or system.

[para 41] The Supreme Court of Canada's test discussed with respect to the application of section 18(1)(a) applies here as well. There must be a reasonable expectation of probable harm, and the Public Body must provide sufficient evidence to show that the likelihood of any of the above scenarios is "considerably above" a mere possibility.

[para 42] In *Canada (Information Commissioner) v. Canada (Prime Minister)*, 1992 CanLII 2414 (FC), [1992] F.C.J. No. 1054, Rothstein J., as he then was, made the following observations in relation to the evidence a party must introduce in order to establish that harm will result from disclosure of information. He said (emphasis added):

> While no general rules as to the sufficiency of evidence in a section 14 case can be laid down, what the Court is looking for is support for the honestly held but perhaps subjective opinions of the Government witnesses based on general references to the record. Descriptions of possible harm, even in substantial detail, are insufficient in themselves. <u>At the least, there must be a clear and direct linkage between the disclosure of specific information and the harm alleged. The Court must be given an explanation of how or why the harm alleged would result from disclosure of specific information.</u> If it is self-evident as to how and why harm would result from disclosure, little explanation need be given. Where inferences must be drawn, or it is not clear, more explanation would be required. The more specific and substantiated the evidence, the stronger the case for confidentiality. The more general the evidence, the more difficult it would be for a court to be satisfied as to the linkage between disclosure of particular documents and the harm alleged.

[para 43] The "harm test" must be applied on a record-by-record basis (Orders F2002-024, at para. 36, F2009-009, at para. 91).

[para 44] The Public Body states that the disclosure of this information could create significant security concerns, and would compromise the integrity of the system. It states (initial submission, at para. 21):

> 1. The release of the computer path ways, the server's name and internal URL would have a causal connection. The record very clearly identifies the number of the computer which stores the information. Revealing this information to the general public would have adverse effects, including but not limited to allowing cyber attackers/hackers to disrupt communication or cause damage to the system application.
> 2. The release of the computer system identification numbers would provide cyber attackers/hackers the means to remotely execute random code on the application and possibly even elevate their privileges to allow them to gain full and complete access to the application. This would result in the system being corrupted and cause significant harm to the law enforcement institutions who use it and to law enforcement in general.
> 3. There is a reasonable expectation that the harm will occur if computer identification number fell into the public domain, this could permit an unauthorized user to gain access to the network or computer system which result to significant harm such as destroy important Public Body's data and render a workstation or server unable to function.

[para 45] I accept this explanation, and the Public Body's application of this provision to the minimal amount of information to which it was applied.

Exercise of discretion

[para 46] Section 20(1) is a discretionary exception. In *Ontario (Public Safety and Security) v. Criminal Lawyers' Association,* 2010 SCC 23 (CanLII), the Supreme Court of Canada commented on the authority of Ontario's Information and Privacy Commissioner to review a head's exercise of discretion.

[para 47] The Supreme Court of Canada confirmed the authority of the Information and Privacy Commissioner of Ontario to quash a decision not to disclose information pursuant to a discretionary exception and to return the matter for reconsideration by the head of a public body. The Court also considered the following factors to relevant to the review of discretion:

- the decision was made in bad faith
- the decision was made for an improper purpose
- the decision took into account irrelevant considerations
- the decision failed to take into account relevant considerations

[para 48] In Order F2010-036 the adjudicator considered the application of the above decision of the Court to Alberta's FOIP Act, as well as considered how a public body's exercise of discretion had been treated in past orders of this Office. She concluded (at para. 104):

> In my view, these approaches to review of the exercise of discretion are similar to that approved by the Supreme Court of Canada in relation to information not subject to solicitor-client privilege in *Ontario (Public Safety and Security)*.

[para 49] In *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2020 ABQB 10 (CanLII) (*EPS*), the Court provided detailed instructions for public bodies exercising discretion to withhold information under the Act. This decision was issued after the Public Body provided its submissions to this inquiry. However, it might be helpful for the Public Body to review the discussion.

[para 50] The Court said (at para. 416)

> What *Ontario Public Safety and Security* requires is the weighing of considerations "for and against disclosure, including the public interest in disclosure:" at para 46. The relevant interests supported by non-disclosure and disclosure must be identified, and the effects of the particular proposed disclosure must be assessed. Disclosure or non-disclosure may support, enhance, or promote some interests but not support, enhance, or promote other interests. Not only the "quantitative" effects of disclosure or non-disclosure need be assessed (how much good or ill would be caused) but the relative importance of interests should be assessed (significant promotion of a lesser interest may be outweighed by moderate promotion of a more important interest). There may be no issue of "harm" in the sense of damage caused by disclosure or non-disclosure, although disclosure or non-disclosure may have greater or lesser benefits. A reason for not disclosing, for example, would be that the benefit for an important interest would exceed any benefit for other interests. That is, discretion may turn on a balancing of benefits, as opposed to a harm assessment.

[para 51] It further explained the weighing of factors at paragraph 419:

> …If disclosure would enhance or improve the public body's interests, there would be no reason not to disclose. If non-disclosure would benefit the public body's interests beyond any benefits of disclosure, the public body should not disclose. If disclosure would neither enhance nor degrade the public body's interests, given the "encouragement" of disclosure, disclosure should occur. Information should not be disclosed only if it would run counter to, or degrade, or impair, that is, if it would "harm" identified interests of the public body.

[para 52] Lastly, the Court described burden of showing that discretion was properly exercised (at para. 421):

> I accept that a public body is "in the best position" to identify its interests at stake, and to identify how disclosure would "potentially affect the operations of the public body" or third parties that work with the public body: EPS Brief at para 199. But that does not mean that its decision is necessarily reasonable, only that it has access to the best evidence (there's a difference between having all the evidence and making an appropriate decision on the evidence). The Adjudicator was right that the burden of showing the appropriate exercise of discretion lies on the public body. It is obligated to show that it has properly refrained from disclosure. Its reasons are subject to review by the IPC. The public body's exercise of discretion must be established; the exercise of discretion is not

presumptively valid. The public body must establish proper non-disclosure. The IPC does not have the burden of showing improper non-disclosure.

[para 53] The Public Body states that it reviewed the Court's discussion in *EPS*, and concluded that it would continue to withhold information under section 20(1)(m). It states that it considered factors weighing against disclosure, such as:

- the harm that could result from disclosure;
- whether the Applicant's access request could be satisfied by severing the information and providing as much information as possible to the Applicant;
- whether the disclosure of the information would increase public confidence in the operation of the Public Body.

[para 54] The Public Body also considered whether disclosure of the information would be in the public interest, using the criteria set out for determining whether fees should be waived in the public interest (under section 93(4)(b)).

[para 55] I accept that the Public Body considered the appropriate factors in exercising its discretion to withhold information under section 20(1).

3. Did the Public Body properly apply section 21(1) of the Act (disclosure harmful to intergovernmental relations) to the information in the records?

[para 56] Section 21(1) states:

> *21(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 relations between the Government of Alberta or its agencies and any of the following or their agencies:*
>
> *(i) the Government of Canada or a province or territory of Canada,*
>
> *(ii) a local government body,*
>
> *(iii) an aboriginal organization that exercises government functions, including*
>
> *(A) the council of a band as defined in the Indian Act (Canada), and*
>
> *(B) an organization established to negotiate or implement, on behalf of aboriginal people, a treaty or land claim agreement with the Government of Canada,*
>
> *(iv) the government of a foreign state, or*
>
> *(v) an international organization of states,*
>
> *or*
>
> *(b) reveal information supplied, explicitly or implicitly, in confidence by a government, local government body or an organization listed in clause (a) or its agencies.*

[para 57] Section 21(1) addresses intergovernmental relations. Section 21(1)(b) applies to information that was supplied to a public body by a government, local government body, or organization listed in section 21(1)(a), or one of its agencies. The Public Body may withhold information if either section 21(1)(a) or (b) apply to that information.

[para 58] In Order F2004-018, the former Commissioner stated that four criteria must be met before section 21(1)(b) applies:

> There are four criteria under section 21(1)(b) (see Order 2001-037):
>
> a) the information must be supplied by a government, local government body or an organization listed in clause (a) or its agencies;
>
> b) the information must be supplied explicitly or implicitly in confidence;
>
> c) the disclosure of the information must reasonably be expected to reveal the information; and
>
> d) the information must have been in existence in a record for less than 15 years.

[para 59] This test has been applied in subsequent Orders (see Order F2009-038 at para. 74-75, which also addressed EPS as the public body applying the provision).

[para 60] Past Orders of this Office have cited the following factors in determining whether a third party supplied information in confidence:

> 1. communicated to the public body on the basis that it was confidential and that it was to be kept confidential;
> 2. treated consistently in a manner that indicates a concern for its protection from disclosure by the affected person prior to being communicated to the public body;
> 3. not otherwise disclosed or available from sources to which the public has access;
> 4. prepared for a purpose which would not entail disclosure.

(See Orders 99-018, F2008-017). This test was upheld by the Court of Queen's Bench in *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2012 ABQB 595 (at para. 41).

[para 61] The Public Body applied section 21(1)(b) to a few sentences, which were repeated several times in the records (on pages 42, 49, 51, 56, 59 and 90). The Public Body states that this information was provided by the Calgary Police Service (CPS). It states that CPS is a local government body listed in section 21(1)(a), and that the information was supplied in confidence. The Public Body also states that disclosure would reveal the information that was supplied, and that the information was in existence for less than 15 years.

[para 62] A "local government body" is defined in section 1(i) of the FOIP Act, and includes police services as defined in the *Police Act*. CPS is a police service defined in

the *Police Act*. Therefore, the information withheld under section 21(1)(b) is information supplied by a local government body.

[para 63] However, past Orders of this Office call into question whether CPS can supply information to the Public Body within the terms of section 21(1)(b). In Order F2009-027, the adjudicator considered whether an RCMP detachment, when contracted to provide policing services to the City of St. Albert, could supply information to the Public Body (then Alberta Justice and Attorney General) within the terms of section 21(1)(b). She considered whether the RCMP detachment was a federal agency when acting as a municipal police service and determined that it was not.

[para 64] She concluded that the RCMP detachment was a police service as defined in section 1(l)(iv) of the *Police Act*.

[para 65] However, the adjudicator also concluded (at paras. 42-44):

> Further, under section 2 of the *Police Act*, a police service acts under the direction of either the Solicitor General and Public Safety or the Minister of Justice and Attorney General when carrying out official duties. Consequently, the exchange of information between an RCMP detachment and the Minister of Justice and Attorney General under the *Police Act* is intragovernmental in nature, rather than intergovernmental. I find that when the RCMP supplied information to the Public Body, it acted as an entity representing the Government of Alberta, and acted under the direction of the Government of Alberta.
>
> The question remains whether section 21(1)(b) encompasses information supplied by a representative of the Government of Alberta, as I have found the RCMP detachment to be. As discussed in Order F2008-027, the use of the phrase "a government, local government body, or organization *listed* in clause (a)" as opposed to a more general phrase such as "a government, local government body referred to in clause (a)," or simply "a government, local government body, or organization in clause (a)," means that a specific list in clause (a) is being referred to in clause (b). I interpret subclauses (i) – (v) in section 21(1)(a) as creating a list of entities belonging to a single, identifiable class: those entities with whom the Government of Alberta's relations are to be protected from harm. The Government of Alberta is not included in the list in subclauses (i) – (v), presumably because there is no need to protect the Government of Alberta's relations with itself.
>
> I find that the Government of Alberta it is not a government listed in clause (a) for the purposes of section 21(1)(b). As a result, information supplied by RCMP acting as agent for the Solicitor General or the Minister of Justice and Attorney General is not subject to section 21(1)(b).

[para 66] The adjudicator determined that the RCMP detachment was acting as a representative of the Public Body, and therefore as a representative of the Government of Alberta. She concluded that when the RCMP detachment supplied information to the Public Body, the Public Body was essentially supplying information to itself. Therefore, section 21(1)(b) could not apply.

[para 67] This analysis was adopted in Order F2020-17, which also related to an RCMP detachment acting as a provincial police service. This latter Order was upheld in *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2021 ABQB 304. Order F2020-17 and the Court decision focus primarily on whether the RCMP detachment were acting as a federal agency for the purpose of section 21(1)(b).

[para 68] The analysis in Order F2009-027 seems also to apply to a municipal police service, such as CPS. In that Order, the adjudicator found that *all police services* act under the direction of the Minister of Justice and Solicitor General (then the Minister of Justice and Attorney General) with respect to the administration of justice. Therefore, when a police service, as defined in the *Police Act*, supplies information relating to the administration of justice to the Public Body, it is acting under the direction of the Minister and the information is essentially flowing from the Public Body to the Public Body.

[para 69] CPS is a police service within the definition in the *Police Act*, which states:

> *1(l) "police service" means*
>
> *(i) a regional police service;*
>
> *(ii) a municipal police service;*
>
> *(iii) the provincial police service;*
>
> *(iv) a police service established under an agreement made pursuant to section 5;*

[para 70] The FOIP Act accordingly defines CPS as a "local government body":

> *1(p) "public body" means*
>
> *...*
>
> *(vii) a local public body,*
>
> *1(j) "local public body" means*
>
> *...*
>
> *(iii) a local government body;*
>
> *1(i) "local government body" means*
>
> *...*
>
> *(x) any*
>
> *(A) commission,*
>
> *(B) police service, or*
>
> *(C) policing committee,*
>
> *as defined in the Police Act,*

[para 71] Section 2 of the *Police Act* states:

> *2(1) The Minister is charged with the administration of this Act.*
>
> *(2) Notwithstanding anything in this Act, all police services and peace officers shall act under the direction of the Minister of Justice and Solicitor General in respect of matters concerning the administration of justice.*

[para 72] The result is that CPS is a "local government body" within the terms of section 21(1)(a)(ii), but is also acting under the direction of the Minister of the Public Body with respect to the administration of justice.

[para 73] In Order F2008-027, the adjudicator agreed that the Edmonton Police Service is a local government body within the terms of section 21(1)(a)(ii). However, she also noted (at para. 91):

> The authority to establish a municipal police service also lies in the *Police Act*, and the powers and duties of a provincial police service are established by the legislation. Consequently, when a government, local government body or organizations listed in clause (a) [or] its agencies supplies information to it in order for it to perform its policing function, it can be argued that the Public Body receives the information on behalf of the Government of Alberta.

[para 74] The public body in Order F2020-17 (Edmonton Police Service) has sought an appeal of the Court decision upholding that Order. The analysis regarding a police service's relationship to the Public Body is likely to be directly before the Court of Appeal. Until the Court of Appeal issues a decision on the appeal, the Court's decision in *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2021 ABQB 304 stands. The Court of Appeal may overturn that decision, which could directly affect the outcome of this inquiry on those points. The Court of Appeal may uphold the lower court's decision, leaving the existing precedent the same; the Court of Appeal may also provide clarification regarding how section 21(1)(b) applies to police services supplying information to the Public Body, even in upholding the lower court's decision. In the latter case, comments from the Court of Appeal could also directly affect the outcome of this inquiry.

[para 75] While the Court of Queen's Bench decision stands, knowing that this decision has been appealed and that appeal is underway (although a date for the hearing has not been set) creates some uncertainty regarding the application of the provisions at issue in that case and in this inquiry. In my view, it is better to wait a little longer and have the benefit of any additional guidance the Court of Appeal may provide in the near future.

[para 76] As such, I have decided to retain jurisdiction over the Public Body's application of section 21(1)(b) to the information in the sentences on pages 42, 49, 51, 55, 59 and 90.

Information withheld under section 21(1)(b) substantially similar to information withheld under section 18(1)(a)

[para 77] Despite the above discussion, some of the information withheld by the Public Body under section 21(1)(b) ought to have been withheld under section 18(1)(a). Specifically, the Public Body withheld contact information under section 21(1)(b) (specifically, an email address in the 'to' line in an email) on pages 45 and 48. I note that the email address, phone number and name of the same employee is all withheld under section 21(1)(b) on page 5 of the records, although the Public Body's index of records indicates that it applied only sections 17(1) and 18(1) to information on this page. The Public Body's August 3 *in camera* submission also indicates that the Public Body intended to apply section 21(1) only to the email address of the employee, and not their name on this page. This employee's name has been withheld under section 18(1)(a) in other instances in the records.

[para 78] Regarding the application of section 21(1)(b) to the email address, the Public Body argues that this email address is shared only internally, and only for the purpose of performing work duties.

[para 79] Aside from the question whether CPS can provide information to the Public Body in confidence within the terms of section 21(1)(b), it is difficult to conclude that an email address of a public body employee meets the test for section 21(1)(b), given the purpose of contact information and the usual manner with which contact information is handled vis a vis confidentiality. This is not to say that contact information can never meet the test for section 21)(1)(b); however, the Public Body's submissions on this point – which were provided in an *in camera* submission – are not sufficiently persuasive.

[para 80] I have accepted the Public Body's application of section 18(1) to information identifying various public body employees, including the one to whom this email address relates. It is not clear why the Public Body applied section 21(1)(b) to this email address, and not section 18(1)(a). It is also not clear whether the Public Body intended to apply section 21(1)(b) to the name and contact information of this employee appearing on page 5 of the records (as the records themselves indicate) or if it intended to apply section 18(1)(a) (as the index indicates).

[para 81] In Order F2020-22, I considered a similar situation, in which a public body applied two different exceptions to access to similar information in the records at issue. I said (at paras. 75-80):

> On page 104, the Public Body applied section 20(1) to the first part of a sentence, and section 24(1)(b) to the second part of that sentence. For the reasons provided in the relevant section of this Order, section 24(1) does not apply to the second part of the sentence.
>
> That said, the first and second parts of the sentence both deal with the same subject matter, and reveal the same policing techniques or procedures that are not known to the public. For the reasons above, I accept the Public Body's application of section 20(1) to the information on page 104. For the reasons provided below, I also accept the Public Body's reasons for exercising its discretion to withhold this information.

It would be nonsensical to permit the Public Body to withhold the first part of the sentence under section 20(1) and order it to disclose the second part of the sentence. Disclosing the second part of the sentence would undermine the purpose of withholding the first part. Given this, and because the Public Body's arguments regarding the application of section 20(1) clearly apply to the second part of the sentence, I conclude that the Public Body may withhold the information to which it applied section 24(1) on page 104 under section 20(1).

Although rare, this situation is not without precedent. In Order F2008-016, the adjudicator found that the exceptions cited by a public body for withholding certain information did not apply, but that another discretionary exception applied. In that case, the adjudicator cited former Commissioner Order F2004-026, where he said (at para. 52):

> I have noted the Applicant's point that the Public Body cannot have been properly exercising its discretion under a particular provision when it did not even have that provision in mind. I agree that at the time of the initial response, there was a defect in the way the Public Body exercised its discretion, in that it did not have precisely the right provisions in mind for some of the documents. However, as I noted earlier, the principle behind the provisions…was the same for both the provisions initially referenced, and the later ones. This detracts significantly from the idea that the failure to name the right provisions at a particular point in time should preclude the ability to withhold documents in the final result.

The adjudicator applied this reasoning to the facts before her, finding (at para. 149):

> In Order F2004-026, the Commissioner was faced with a situation where the public body raised an exclusion late in the process and not at the time of the initial response to the Applicant. I understand that allowing the EPS to withhold information under section 27(1)(b) and 27(1)(c) of the Act takes this analysis a step further, but I feel it is appropriate to do so in these limited circumstances, for the same principles as those on which the Commissioner relied on in Order F2004-026.

This rationale applies in this case as well, as the Public Body's reasons for applying section 20(1) to one part of the sentence apply equally to the second part withheld under section 24(1).

[para 82] In my view, this rationale applies in this case as well. The contact information of the public body employee withheld under section 21(1)(b) could identify that employee. I have accepted that this employee's name can be withheld under section 18(1)(a), for the reasons given in that section of this Order. It would be nonsensical to accept the application of section 18(1)(a) to withhold the names of certain public body employees, but order the disclosure of their contact information (and in one instance, the name of the employee) that was withheld under a different provision. I have also considered that the Public Body has cited similar reasons for withholding the information

under the different provisions (in this case, safety concerns), and that I have accepted the Public Body's arguments regarding the harm to safety or health that could reasonably be expected to result from disclosure under section 18(1)(a). In other words, because I have accepted that the disclosure of certain public body employee names could reasonably be expected to threaten their health or safety, it is illogical to order the disclosure of other information that is sufficiently similar so as to have the same effect from disclosure.

V. ORDER

[para 83] I make this Order under section 72 of the Act.

[para 84] I find that the Public Body properly applied section 18(1)(a) to the information in the records.

[para 85] I find that the Public Body can withhold the information described at paragraph 77 of this Order under section 18(1)(a).

[para 86] I find that the Public Body properly applied section 20(1)(m) to information in the records.

[para 87] I am retaining jurisdiction regarding the Public Body's application of section 21(1)(b) (except the information described at paragraph 77 of this Order), pending the appeal of *Edmonton Police Service v. Alberta (Information and Privacy Commissioner)*, 2021 ABQB 304.

_____

Amanda Swanek
Adjudicator