ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2024-41

November 29, 2024

PUBLIC SERVICE COMMISSION

Case File Number 027129

Office URL: www.oipc.ab.ca

Summary: The Applicant is an employee of the Government of Alberta. The Applicant made an access request under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act) to the Public Service Commission (the Public Body) for information regarding an application she had made for vaccination exemption status.

The Public Body located responsive records, but severed information from them under sections 17(1) (disclosure harmful to personal privacy), 18 (disclosure harmful to individual or public safety), 19 (confidential evaluations), 20 (disclosure harmful to law enforcement), 24 (advice from officials) and 25 (disclosure harmful to the economic and other interests of a public body).

The Adjudicator found that there was insufficient evidence to support the Public Body's severing decisions. She found that the Public Body was not authorized or required by the FOIP Act to withhold information from the Applicant and directed the Public Body to give the Applicant access to all the information it had severed from the records.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act,* R.S.A. 2000, c. F-25, ss. 1, 17, 18, 19, 20, 24, 25, 72

Authorities Cited: AB: Orders F2004-029, F2013-51, F2015-29, F2020-08, F2021-28, F2022-62

Cases Cited: *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner),* 2014 SCC 31 (CanLII)

I. BACKGROUND

[para 1] The Applicant made an access request to the Public Service Commission (the Public Body) for the following information:

> All formal and Informal written correspondence, voice mails, phone TEXTS, WORD or PDF documents, IMAGES, VIDEO and reference material. Including Internal and external communication, guidelines, policies, legal opinions and directives of the Vaccination Exemption Team that provide support rational and/or articulate adjudication discussions and all interpersonal communication of the decision makers inclusive of any GOA employee or representative whether or not a part of the Vaccination Exemption team - that influenced or contributed to my specific exemption application. Plus the names of all persons, whether or not employees, supervisors or managers of the GOA, who were provided my exemption application information, vaccination status, vaccination disclosure, IGX vaccination details, or any other medical or testing information.

[para 2] The Public Body responded to the Applicant on May 16, 2022. The Public Body severed information from the records under sections 17, 18, 19, 20, 24, and 25 of the FOIP Act.

[para 3] The Applicant requested review by the Commissioner of the Public Body's severing decisions. The Commissioner authorized mediation. At the conclusion of this process, the Applicant requested an inquiry. The Commissioner agreed to conduct the inquiry and delegated her authority to conduct it to me.

II. ISSUES:

ISSUE A: Does section 17(1) (disclosure harmful to personal privacy) of the FOIP Act require the Public Body to withhold personal information from the Applicant?

ISSUE B: Does section 18 (disclosure harmful to individual or public safety) of the FOIP Act authorize the Public Body to withhold information from the Applicant?

ISSUE C: Does section 19(2) (confidential evaluations) of the FOIP Act authorize the Public Body to withhold information from the Applicant?

ISSUE D: Does section 20(1) (disclosure harmful to law enforcement) of the Act authorize the Public Body to withhold information from the Applicant?

ISSUE E: Does section 24(1) (advice from officials) of the FOIP Act authorize the Public Body to withhold information from the Applicant?

ISSUE F: Does section 25(1) of the Act (disclosure harmful to economic and other interests of a public body) authorize the Public Body to withhold information from the Applicant?

III. DISCUSSION OF ISSUES

ISSUE A: Does section 17(1) (disclosure harmful to personal privacy) of the FOIP Act require the Public Body to withhold personal information from the Applicant?

[para 4] Section 17 states, in part:

> *17(1) The head of 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.*
>
> *[...]*

[para 5] If records contain the personal information of a third party as defined in section 1(r) of the FOIP Act, and disclosure of the personal information would be an unreasonable invasion of personal privacy, then section 17(1) requires a Public Body to disclose the information.

[para 6] Section 1(r) of the FOIP Act defines "third party" for the purposes of the FOIP Act as "a person, a group of persons or an organization other than an applicant or a public body".

[para 7] The Public Body severed the names of employees involved in making decisions regarding the Applicant's application for a vaccination exemption where these names appear in the records.

[para 8] The Public Body prefaced its submissions with the following:

> As a preface to all arguments below, it is very important to note that all of the responsive records are related to the Covid pandemic. During the Covid pandemic, Albertans were faced with the immense stressors and pressure associated with a global pandemic. Differing personal beliefs and views on pertinent issues resulted in unprecedented strife amongst friends, families and community members, and this tension undoubtedly permeated into the workplace. Many Albertans did not agree with the government's actions during the pandemic and were very angry and abusive towards government employees. This abuse included death threats.
>
> Because of this, a cautious approach was taken. In situations where we would normally release a government employee's name and contact information, we have severed them in order to protect them from threats of harm that have been clearly documented in the news and continue to be an issue with continuing protests and demonstrations.
>
> We have also severed workplace addresses as there have been incidents of individuals showing up to government offices to protest the government's actions during the pandemic.

> Releasing records to an individual is releasing them to the public. Once released from the government's control, we cannot influence where they may end up. If the names and contact information of government employees who were involved in decision-making surrounding Covid pandemic issues were released to the public, there is a real chance that they could be subject to harm and abuse from the public.

[para 9] With regard to its decision to apply section 17(1) to the names of employees, the Public Body states:

> Section 17 (disclosure harmful to personal privacy) of the Act states:
>
> > The head of 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.
>
> Pages 5, 7, 38, 40–41, 43, 47, 59, 62–65, 67, 74–76, 78–79, 83, 88–89, 94, 102, 108, and 111: Section 17(1) was applied to the employees of the Government of Alberta (GoA) who were working on Covid pandemic related issues. As stated above, there is a real possibility of harm to these individuals, and therefore their names and contact information have been severed so as to limit their exposure to threats of harm. This type of information would normally be released as it is part of the employees' responsibilities to respond to the public and to be accountable for these actions. However, we are of the view that the highly charged and controversial nature of the Covid pandemic and government's response has added a personal element to the involvement of these individuals. The line between work and personal life has been blurred by certain members of the public who have attacked government workers outside of work and have used this type of personal information to threaten these employees.
>
> As such, the GoA confirms our position that section 17 applies to names and contact information of GoA employees in the context of this request.

[para 10] The Public Body's position is that section 17(1) requires it to withhold the names and identifying information of employees to ensure their safety.

[para 11] Section 17 of the FOIP Act requires a public body to withhold the personal information of identifiable individuals if disclosing the information would be an unreasonable invasion of personal privacy.

[para 12] Past orders of this office have held that section 17(1) does not apply to information about persons acting in a representative capacity that lacks a personal dimension.

[para 13] In Order F2013-51, the Director of Adjudication distinguished personal information from information about a third party acting as a representative. She said:

> As well, the Public Body has severed information, partly in reliance on section 17, that may be properly characterized as 'work product'. For example, it has severed the questions asked by an investigator, in addition to the answers of those interviewed. It has also withheld what is possibly a line of inquiry which the investigator means to follow (the note severed from record 1-151). While some of the questions and notes may reveal the personal information of witnesses, it does not appear that it is always the case that they do, and it appears possible that the Public Body withheld information on the basis that it may reveal something about the investigator performing duties on its behalf, rather than personal information about third parties.

The Public Body has also withheld notes of an interview by the Public Body's investigator of the University of Calgary's legal counsel, in part in reliance on section 17. Information about the legal counsel's participation in the events surrounding the Applicant's complaint to the University is not her personal information unless it has a personal aspect, which was not shown.

As well, it may be that some of the information of persons interviewed in the third volume relating to the Applicant's 'retaliation' complaint, which was withheld in reliance on section 17, may be information about events in which these persons participated in a representative rather than a personal capacity. Again, to be personal in such a context, information must be shown to have a personal dimension.

In Order F2009-026, the Adjudicator said:

> If information is about employees of a public body acting in a representative capacity the information is not personal information, as the employee is acting as an agent of a public body. As noted above, the definition of "third party" under the Act excludes a public body. In Order 99-032, the former Commissioner noted:
>
> The Act applies to public bodies. However, public bodies are comprised of members, employees or officers, who act on behalf of public bodies. A public body can act only through those persons.
>
> In other words, the actions of employees acting as employees are the actions of a public body. Consequently, information about an employee acting on behalf of a public body is not information to which section 17 applies, as it is not the personal information of a third party. If, however, there is information of a personal character about an employee of a public body, then the provisions of section 17 may apply to the information. I must therefore consider whether the information about employees in the records at issue is about them acting on behalf of the Public Body, or is information conveying something personal about the employees.

In that case, the Adjudicator found that information solely about an employee acting as a representative of a public body was information about the public body, and not information about the employee as an identifiable individual. In Mount Royal University v. Carter, 2011 ABQB 28 (CanLII), Wilson J. denied judicial review of Order F2009-026.

In Order F2011-014, the Adjudicator concluded that the name and signature of a Commissioner for Oaths acting in that capacity was not personal information, as it was not information about the Commissioner for Oaths acting in her personal capacity. She said:

> Personal information under the FOIP Act is information about an identifiable individual that is recorded in some form.
>
> However, individuals do not always act on their own behalf. Sometimes individuals may act on behalf of others, as an employee does when carrying out work duties for an employer. In other cases, an individual may hold a statutory office, and the actions of the individual may fulfill the functions of that statutory office. In such circumstances, information generated in performance of these roles may not necessarily be about the individual who performs them, but about the public body for whom the individual acts, or about the fulfillment of a statutory function.
>
> I find that the names and other information about employees of the Public Body and the University of Calgary acting in the course of their duties, as representatives of their employers, cannot be withheld as personal information, unless the information is at the same time that of an individual acting in the individual's personal capacity.

[para 14] From the foregoing, I conclude that information about an employee acting in a representative capacity will not be personal information to which section 17(1) applies, unless the information has a personal dimension. When an employee acts on behalf of a public body, the employee is not acting as a "third party" within the terms of section 17(1), but as the public body.

[para 15] In cases where the context in which information appears does not support finding that it has a personal dimension, it must be proven, with evidence, that the information does possess this quality.

[para 16] The information severed by the Public Body under section 17(1) consists of the names and contact information of employees acting in a representative capacity. There is nothing in the records to suggest that they acted in capacities other than as representatives of public bodies when they wrote emails or took steps. The Public Body has not provided any evidence that would support finding that the employees acted in anything other than their professional capacities. Given that the Applicant's access request is for details of an employment decision that was made regarding her application, it is very unlikely that the employees referenced in the records acted in their private capacities as citizens when making the decision. On the contrary, they would have no authority to handle information or make decisions in their private capacities.

[para 17] The Public Body's submissions indicate that it applied section 17 of the FOIP Act as it was concerned about the safety of employees should information revealing their contact information and role in making decisions be disclosed. The Public Body also applied section 18 of the FOIP Act, which addresses disclosure harmful to individual and public safety, to the names and identifying information of employees. Section 18 is the appropriate provision to apply when a public body has concerns about employee safety if information is disclosed. While there can be cases where both section 17 and 18 apply to the same information, when there is no personal dimension to information, only section 18 can apply. This point is made in Order F2019-09 at paragraph 31.

[para 18] I will address the Public Body's concerns regarding employee safety when I address its severing under section 18. To conclude, I find that section 17(1) does not require the Public Body to withhold the information to which it applied this provision from the Applicant.

ISSUE B: Does section 18 (disclosure harmful to individual or public safety) of the FOIP Act authorize the Public Body to withhold information from the Applicant?

[para 19] Section 18 of the FOIP Act states, in part:

> *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, or

(b) interfere with public safety.

[…]

[para 20] The Public Body applied section 18 to withhold information about its employees. The Public Body argues:

> Section 18 (disclosure harmful to individual or public safety) of the Act states: 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, or (b) interfere with public safety. Pages 5, 7, 38, 40–41, 43, 47, 59, 62–65, 67, 74–76, 78–79, 83, 88–89, 94, 102, 108, and 111: Section 18(1) was also applied to the employees of the Public Body who were working on Covid pandemic related issues. The public knowledge of the physical addresses, email addresses, and contact information of GoA staff members who were working on Covid pandemic related issues has been utilized by people who have made serious threats of physical harm and have shown up at the work locations of GoA staff members. The threats that have been made are extreme and have included death threats to GoA staff and, in some cases, their families.
>
> The Vaccination Exemption Requests (VER) team members were told that they should be ashamed of themselves, and that the work they were doing was revolting. This type of harassment has a significant impact on the psychological well-being and mental health of these GoA employees, which was only compounded with the immense stressors already present during the Covid pandemic. These employees were simply carrying out their job responsibilities, regardless of their own personal beliefs. The VER team members were asked where they live, whether they have family or children, and what their religious beliefs are. These types of questions are deeply personal, and show a pattern of conflict and stress within the workplace that threatened the mental health of employees on a personal level.
>
> The VER team members were assured that their personal information would be kept confidential in light of the controversial and divisive nature of Covid pandemic related issues. Alberta's Occupational Health and Safety legislation requires employers to do everything they reasonably can to protect the health and safety of their employees, and the Public Body determined that protecting the identity of the VER team members during this unprecedented period of tension was required to meet their obligations.
>
> The makeup of these decision-making panels was not widely shared, even amongst PSC itself. Measures were taken to protect the panels and their members including all communications being moved to generic shared email accounts and not revealing the identities of staff working in these positions, even amongst GoA staff.
>
> The Public Body employees' contact information, who were working on Covid pandemic related issues, has therefore been protected as a reasonable expectation of harm follows its disclosure. In the exercise of utmost caution, this information should also not be released because of the distinct possibility of harassment by means of email and phone calls that could also harm employee's safety and mental health.

[para 21] Section 18 applies to information the disclosure of which may be reasonably expected to result in harm to an individual or to the public.

[para 22] In *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner),* 2014 SCC 31 (CanLII), the Supreme Court of Canada confirmed that when access and privacy statutes refer to reasonable expectations of harm, a party seeking to rely on the exception must demonstrate that disclosure will result in a risk of harm that is beyond the merely possible or speculative. The Court stated:

> It is important to bear in mind that these phrases are simply attempts to explain or elaborate on identical statutory language. The provincial appellate courts that have not adopted the "reasonable expectation of probable harm" formulation were concerned that it suggested that the harm needed to be probable: see, e.g., Worker Advisor, at paras. 24-25; *Chesal v. Nova Scotia (Attorney General),* 2003 NSCA 124 (CanLII), 219 N.S.R. (2d) 139, at para. 37. As this Court affirmed in *Merck Frosst*, the word "probable" in this formulation must be understood in the context of the rest of the phrase: there need be only a "reasonable expectation" of probable harm. The "reasonable expectation of probable harm" formulation simply "captures the need to demonstrate that disclosure will result in a risk of harm that is well beyond the merely possible or speculative, but also that it need not be proved on the balance of probabilities that disclosure will in fact result in such harm": para. 206.
>
> Understood in this way, there is no practical difference in the standard described by the two reformulations of or elaborations on the statutory test. 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 in original.]
>
> This Court in *Merck Frosst a*dopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expect 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 23] Section 18 employs the phrase "could reasonably be expected to". Accordingly, the onus is on the Public Body to establish, with evidence, that it has a reasonable expectation of probable harm resulting from disclosure.

[para 24] The Public Body asserts that employees who made decisions regarding vaccination exemptions for other employees were told they should be ashamed of themselves and that their work was "revolting". The Public Body does not provide the

source of its information. It is unclear from its account who referred to the work of the Public Body's employees as "revolting" – its employees or members of the public – or in what context the remark(s) was made. It is unknown whether the comment was made once, or more than once, or whether it was directed at a particular employee or made generally. The Public Body does not explain how any such remarks were communicated, or how the Public Body knows the remark was made.

[para 25] The Public Body does not indicate whether it took any action in relation to the remarks it alleges were made, in its role as employer, other than determining that it would not release the identities or contact information of employees. It does not indicate that it instituted a communications protocol in relation to the makers of the remarks it asserts were made. If the maker of the remarks was an employee of the Government of Alberta, it does not indicate that it exercised management rights as a consequence of the remarks.

[para 26] Accepting that the remark (or remarks) was made, I am unable to say that it would pose a risk of psychological harm if similar remarks are made. Prior orders of this office have stated: "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" (See Order F2004-029 at paragraph 23).

[para 27] As the Public Body did not support its assertions with evidence, it is unclear that the remark the Public Body asserts was made constitutes harassment. It is also unclear that releasing the information to which the Public Body applied section 18 could reasonably be expected to result in additional comments of the kind described by the Public Body being made.

[para 28] In finding that the Public Body has not supported its application of section 18 with adequate evidence, I note that the Adjudicator in Order F2020-08 summarized the kinds of evidence that assist a decision maker to determine that the terms of section 18 are met. She said at paragraphs 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 29] I have been provided with insufficient evidence to establish that the direct lines, email addresses, and cell phones of employees have been used to harass employees.

[para 30] To conclude, I find that the Public Body has not established that section 18 authorizes withholding information in the records from the Applicant.

ISSUE C: Does section 19(2) (confidential evaluations) of the FOIP Act authorize the Public Body to withhold information from the Applicant?

[para 31] Section 19 states:

> *19(1) The head of a public body may refuse to disclose to an applicant personal information that is evaluative or opinion material compiled for the purpose of determining the applicant's suitability, eligibility or qualifications for employment or for the awarding of contracts or other benefits by a public body when the information is provided, explicitly or implicitly, in confidence.*
>
> *(2) The head of a public body may refuse to disclose to an applicant personal information that identifies or could reasonably identify a participant in a formal employee evaluation process concerning the applicant when the information is provided, explicitly or implicitly, in confidence.*
>
> *(3) For the purpose of subsection (2), "participant" includes a peer, subordinate or client of an applicant, but does not include the applicant's supervisor or superior.*

[para 32] The Public Body applied section 19(2) to records 72 and 73. Records 72 and 73 contain a panel decision regarding the Applicant's application and the reasons for it.

[para 33] The Public Body argues:

> Section 19 (confidential evaluation) of the Act states: (2) The head of a public body may refuse to disclose to an applicant personal information that identifies or could reasonably identify a

participant in a formal employee evaluation process concerning the applicant when the information is provided, explicitly or implicitly, in confidence.

Pages 72–73: Section 19(2) was applied to the minutes of a formal evaluation process conducted by the adjudication panel participants. The information was provided, explicitly or implicitly, in confidence, and in this very sensitive Covid pandemic situation, the disclosure of the information could reasonably identify the participants.

[para 34] The Public Body severed records 72 and 73 in their entirety on the basis of section 19(2).

[para 35] Section 19(2) applies to *personal* information that would reveal the identities of participants in an employee evaluation (other than supervisors or superiors of an employee). Records 72 and 73 do not refer to an assessment of the Applicant as an employee, but a decision whether she was entitled to a vaccination exemption. Moreover, there is no personal information in the decision except that of the Applicant, and that information does not identify a "participant" within the terms of section 19(2) and cannot reasonably be expected to do so.

[para 36] To conclude, I find that the information severed under section 19(2) does not meet the terms of this provision.

ISSUE D: Does section 20(1) (disclosure harmful to law enforcement) of the Act authorize the Public Body to withhold information from the Applicant?

[para 37] The Public Body applied section 20(1)(m) of the FOIP Act to cell phone numbers where these appear on records 7, 50, 63-64, 74-76, 78-79, 83, and 88-89.

[para 38] Section 20(1)(m) of the FOIP Act 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 39] The Public Body argues:

> Section 20 (disclosure harmful to law enforcement) of the Act states: (1)(m) harm the security of any property or system, including a building, a vehicle, a computer system, or a communications system.
>
> Pages 7, 50, 63-64, 74-76, 78-79, 83, 88-89: Section 20(1)(m) protects the disclosure of information that would "harm the security of any property or system, including… a communications system." Certain cell phone numbers belonging to Government of Alberta employees are unlisted for security reasons. Disclosing this information would jeopardize the safety of our communications system. Were this information disclosed, the safety of our communications system would be at risk and new unlisted numbers would have to be obtained.

[para 40] From my review of the records, I understand that the Public Body severed cell phone numbers of employees where these appear in the records. The cell phone numbers appear to be information that populates automatically when an employee sends an email.

[para 41] In Order F2021-28 I rejected the argument that disclosing a cell phone number could reasonably be expected to harm property or a system. I said:

> It is unclear to me that section 20(1)(m) applies in the situation described in Order F2020-13, although I agree that cell phone numbers should be withheld for the reasons set out in Order F2020-13. Section 20(1)(m), reproduced above, applies to information that will harm the security of property or a system, including a building, vehicle, computer system or a communications system, if it is disclosed. While I agree that a cell phone or direct line is part of a communications system, I am unable to see how disclosing a direct line or cell phone number could harm the security of the Public Body's communications system, particularly when disclosing a general number, such as that on the police officer's business card, does not. If the disclosure of a cell phone or direct line number alone could be expected to harm the security of a communications system, an explanation is required as to how this result may reasonably be anticipated. In addition, it seems to me that there are potential harms to a public body when a direct line or cell phone is used by members of the public, or even criminal elements, to harass or make inappropriate contact with an employee when the employee is on duty, in addition to being off duty or retired.

[para 42] While the Public Body refers to "certain cell phone numbers" as unlisted for security reasons, the Public Body does not say that the cell phone numbers in the records are unlisted. Given that they are embedded in the emails in the records – that is, they are sent automatically to the recipients of emails -- it is unclear that the cell phone numbers at issue are unlisted.

[para 43] It is also unclear that the cell phone numbers are the Public Body's property or part of a system. Section 20(1)(m) references potential harm to a public body's property or systems. There is no evidence before me that disclosing a cell phone number could reasonably be expected to result in damage to the Public Body's property or systems. It appears unlikely that disclosure of the cell phone number could result in such harm, especially given that the cell phone numbers automatically populate in the signature line in the emails when the employee creates and sends them.

[para 44] I note, too, that the Applicant was the intended recipient of an email on record 85 containing the cell phone number that the Public Body severed elsewhere in the records. For this reason as well, it is uncertain that severing the cell phone numbers serves a purpose.

[para 45] To conclude, I find that the Public Body has not established that section 20(1)(m) authorizes it to withhold information from the records.

ISSUE E: Does section 24(1) (advice from officials) of the FOIP Act authorize the Public Body to withhold information from the Applicant?

[para 46] Section 24 of the FOIP Act states, in part:

24(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to reveal

(a) advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council,

(b) consultations or deliberations involving

(i) officers or employees of a public body,

(ii) a member of the Executive Council, or

(iii) the staff of a member of the Executive Council,

[…]

[para 47] In Order F2015-29, the Director of Adjudication interpreted sections 24(1)(a) and (b) of the FOIP Act and described the kinds of information that fall within the terms of these provisions. She said:

> The intent of section 24(1)(a) is to ensure that internal advice and like information may be developed for the use of a decision maker without interference. So long as the information described in section 24(1)(a) is developed by a public body, or for the benefit or use of a public body or a member of the Executive Counsel, by someone whose responsibility it is to do so, then the information falls under section 24(1)(a).

[para 48] A consultation within the terms of section 24(1)(b) takes place when one of the persons enumerated in that provision solicits information of the kind subject to section 24(1)(a) regarding that decision or action. A deliberation for the purposes of section 24(1)(b) takes place when a decision maker (or decision makers) weighs the reasons for or against a particular decision or action. Section 24(1)(b) protects the decision maker's request for advice or views to assist him or her in making the decision, and any information that would otherwise reveal the considerations involved in making the decision. Moreover, like section 24(1)(a), section 24(1)(b) does not apply so as to protect the final decision, but rather, the process by which a decision maker makes a decision.

[para 49] I agree with the analysis of the Director of Adjudication as to the purpose and interpretation of section 24(1)(a) and agree that this provision applies to information intended to assist a decision maker to make a decision. Section 24(1)(a) protects the policy development process, but not the final decision regarding the policy.

[para 50] In Order F2022-62, the Adjudicator reviewed past orders and identified the kinds of information that have been found not to be subject to section 24(1)(a) or (b). She said:

> In addition to the requirements in those tests, sections 24(1)(a) and (b) apply only to the records (or parts thereof) that reveal substantive information about which advice was sought or

> consultations or deliberations were being held. Information such as the names of individuals involved in the advice or consultations, or dates, and information that reveals only the fact that advice is being sought or consultations held on a particular topic (and not the substance of the advice or consultations) cannot generally be withheld under section 24(1) (see Order F2004-026, at para. 71).
>
> Bare recitation of facts or summaries of information also cannot be withheld under sections 24(1)(a) or (b) unless the facts are interwoven with the advice, proposals, recommendations etc. such that they cannot be separated (Order F2007-013 at para. 108, Decision F2014-D-01 at para. 48).
>
> As well, section 24(1)(a) does not apply to a decision itself (Order 96-012, at para. 31).
>
> The first step in determining whether section 24(1)(a) was properly applied is to consider whether a record would reveal advice, proposals, recommendations, analyses, or policy options (which I will refer to as "advice etc.", section 24(1)(a)); and consultations or deliberations between specified individuals (section 24(1)(b)).

[para 51] The Public Body argues:

> Pages 5, 38, 40, 41, 43, 47, 63-65, 67, 72-76, 78-79, 83, 88-89, 102, 108, 111: Sections 24(1)(a) and (1)(b) were applied to the email exchanges between members of the VER team and emails between PSC employees deliberating advice on the issues related to the Applicant's exemption application. This team was charged with analysing these applications and this involved analysing advice and giving advice to the decision makers on the team so they could properly accept or deny these claims. Also, the information consists of minutes of a formal evaluation process by the adjudication panel participants. The disclosure of the information would compromise the ability of officers of the GoA to freely discuss policy options and provide advice, recommendations, or analyses relating to the Covid pandemic vaccination exemption request.

[para 52] From my review of the records at issue and the Public Body's submissions, I find that the information to which the Public Body applied sections 24(1)(a) and (b) does not fall within the terms of these provisions. At best, the severed information reveals factual questions (record 74) and recitations of facts (record 63). The Public Body also applied section 24(1) to withhold a decision (records 72-73).

Factual Questions

[para 53] While it is true that a decision maker may ask questions in order to make a decision, it is also true that questions may be asked when there is nothing to decide. To put the point differently, the fact that a question is asked does not mean that section 24(1) applies. In this case, I am unable to identify a nexus between the questions asked in the records and a decision to be made. Instead, the questions simply ask about the state of a matter, but do not suggest that the person asking the question had anything to decide on behalf of the Public Body, or that asking the question was intended to assist in deciding anything.

Recitations of Facts

[para 54] As noted above, past orders of this office have held that information that only sets out facts does not fall within the terms of section 24(1). When facts are

presented in such a way as to guide a decision maker as to what to decide, the information may be analysis within the terms of section 24(1)(a). In contrast, when facts are presented solely to inform someone about something that has happened, and there is no indication that the information is intended to guide a course of action, the information will be a "bare recitation of facts",

Decisions

[para 55] As discussed in Order F2015-29, cited above, section 24(1) is intended to protect the process by which a decision is made, but not the decision itself. The decision before me does not contain advice, proposals, recommendations, analyses or policy options or consultation or deliberations as to what the panel should do – it reflects only what the panel decided to do. As such, section 24(1) does not apply.

Conclusion in relation to section 24(1)

[para 56] In concluding that section 24(1) does not authorize the Public Body to withhold information from the Applicant, I acknowledge that the Public Body argues that disclosure of the information to which it applied section 24(1) would "compromise the ability of officers of the GoA to freely discuss policy options and provide advice, recommendations, or analyses relating to the Covid pandemic vaccination exemption requests". As none of the records appear to contain policy options, advice, recommendations or analyses, I am unable to say that disclosure could have this effect.

[para 57] The Public Body did not provide evidence to support its application of 24(1), nor did it speak to each instance of severing. Instead, it left the records to speak for themselves. The records themselves do not support finding that section 24(1) applies.

[para 58] I find that section 24(1) does not apply to the information to which the Public Body applied this provision.

ISSUE F: Does section 25(1) of the Act (disclosure harmful to economic and other interests of a public body) authorize the Public Body to withhold information from the Applicant?

[para 59] The Public Body applied section 25(1)(b) of the FOIP Act to a cell phone number appearing on records 7, 50, 63-64, 74-76, 78-79, 83, 88-89. Section 25 states, in part:]

> *25(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to harm the economic interest of a public body or the Government of Alberta or the ability of the Government to manage the economy, including the following information:*
>
> *[…]*

> *(b) financial, commercial, scientific, technical or other information in which a public body or the Government of Alberta has a proprietary interest or a right of use and that has, or is reasonably likely to have, monetary value;*

[para 60] The Public Body argues:

> Pages 7, 50, 63-64, 74-76, 78-79, 83, 88-89: Section 25(1)(b) has been applied to GoA employee cell phone numbers as the GoA has a proprietary right of use of those numbers. Certain cell phone numbers belonging to Government of Alberta employees are unlisted for security reasons. If they were disclosed in response to a FOIP request, they would more than likely need to be changed. These numbers are not published for a variety of reasons, including to preserve the functionality of the number by preventing unwanted and unsolicited phone calls; to preserve the security of the individual given the number; and to protect the integrity of the communication system of the GoA. As well, if disclosed, it may result in financial loss to the GoA and loss of work time for employees if it is necessary to redeploy their cell phones if the number is compromised for the reasons noted above. It should be noted that section 20(1)(m) is usually applied to unlisted cell phone numbers in conjunction with section 25.

[para 61] The Public Body asserts, without evidence, that the cell phone numbers appearing in the records are not published and are unlisted. It also asserts that the cell phone numbers are "proprietary" as the numbers cannot be assigned to anyone other than the Public Body. It is unknown from its submissions whether the employees referenced in the records continue to work for the Public Body or in what capacity. It is unknown whether the phone numbers in the records continue to be assigned to them.

[para 62] I am unable to accept, without evidence as to the Public Body's contract with its cellular provider, that it has a proprietary interest in phone numbers assigned to its employees or that disclosing cell phone numbers would affect any proprietary interests it may have. It may well be that the Public Body provided the cell phones to employees for their use; however, on the evidence before me it is also possible that the cell phone numbers are the employees' own.

[para 63] I note that one of the phone numbers appearing on record 64 is published in the Government of Alberta directory, so the argument that the phone numbers are "unlisted" is apparently not intended to apply to all the phone numbers in the records, although it appears that section 25 was applied to the listed phone number as well.

[para 64] Section 25 applies to various kinds of proprietary information in which the Government of Alberta or a public body has an interest that have independent monetary value. On the evidence before me, I am unable to agree with the Public Body that cell phone numbers fall within the terms of section 25 of the FOIP Act.

[para 65] Past orders have held that section 25(1)(a) may apply to cell phone numbers if a public body establishes, with evidence, that it may have to expend money or resources to change an assigned phone number as a result of disclosure. (See Order F2021-28 at paragraphs 47 – 53.) In this case, there is no evidence before me that the Public Body would have to expend funds to change phone numbers should the Applicant

receive the requested records. Review of the records reveals that the Applicant received emails containing the information to which the Public Body applied section 25 (record 80). Given that this information was shared with the Applicant, albeit outside the FOIP process, it is unclear why the Public Body refers to the cell phone number as "unlisted".

[para 66] To conclude, I am unable to find that section 25 authorizes the Public Body to withhold information from the Applicant.

IV. ORDER

[para 67] I make this Order under section 72 of the Act. As I find that the Public Body is not authorized or required by the FOIP Act to withhold any information in the records from the Applicant, I order the Public Body to give the Applicant access to the records in their entirety.

[para 68] I order the Public Body to inform me within 50 days of receiving this Order that it has complied with it.

_____
Teresa Cunningham
Adjudicator
/kh